Anomaly Detection Report

Model: autoencoder

Source File: synthetic_logs_1k.csv

Total Anomalies Found: 1000

Total Clusters Detected: 15

Detected Attack Clusters

[DoS] - Severity: High | Confidence: 0.80 | Logs: 6

Reasoning: The cluster of logs shows a high number of HTTP POST requests with a status of 503, indicating a potential denial of service attack.
Common Pattern: The common behavior in this cluster is the repeated occurrence of HTTP POST requests with high response times and status 503.

[Data Exfiltration] - Severity: High | Confidence: 0.80 | Logs: 314

Reasoning: The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.
Common Pattern: The logs exhibit frequent POST requests with unusually large bytes transferred and fast response times to the suspicious destination IP.

[Data Exfiltration] - Severity: High | Confidence: 0.85 | Logs: 516

Reasoning: The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.
Common Pattern: Repeated requests to specific endpoints with varying response times and sizes, all directed towards the same destination IP.

[Data Exfiltration] - Severity: High | Confidence: 0.80 | Logs: 10

Reasoning: The cluster shows a consistent pattern of high response times and anomalous file requests, indicating potential data exfiltration attempts.
Common Pattern: The logs exhibit abnormal file access patterns with high response times, suggesting potential data exfiltration activities.

[HTTP 404 Error Flood] - Severity: High | Confidence: 0.80 | Logs: 21

Reasoning: The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.
Common Pattern: The common behavior in this cluster is the repeated GET requests for specific resources resulting in HTTP 404 errors.

[HTTP 404 Error Flood] - Severity: High | Confidence: 0.80 | Logs: 7

Reasoning: The cluster shows a consistent pattern of multiple HTTP POST requests resulting in 404 errors with high response times, indicating a potential flood attack.
Common Pattern: The common behavior in this cluster is the repeated POST requests to the same endpoint with 404 errors and high response times.

[DoS] - Severity: High | Confidence: 0.80 | Logs: 6

Reasoning: The cluster shows a series of HTTP POST requests with high response times and status code 500, indicating a potential Denial of Service attack.

Anomaly Detection Report

Common Pattern: The attacker is targeting a specific destination IP (0.1.0.1) with multiple POST requests resulting in server errors.

[Data Exfiltration] - Severity: High | Confidence: 0.80 | Logs: 7

Reasoning: The cluster shows a series of HTTP GET requests with high response times and no data transferred, indicating potential data exfiltration attempts.
Common Pattern: The common behavior in this cluster is the retrieval of various resources with no data transfer and high response times.

[DoS] - Severity: High | Confidence: 0.90 | Logs: 12

Reasoning: The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.
Common Pattern: The common behavior in this cluster is multiple requests for the same resource with status code 503 and high response times.

[DDoS] - Severity: High | Confidence: 0.80 | Logs: 17

Reasoning: The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.
Common Pattern: The common behavior in this cluster is multiple requests targeting the same destination IP with consistent response times and status codes.

[DoS] - Severity: High | Confidence: 0.80 | Logs: 19

Reasoning: The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.
Common Pattern: The common behavior in this cluster is the repeated occurrence of POST requests with high response times to the same destination IP.

[HTTP 404 Error Flood] - Severity: High | Confidence: 0.80 | Logs: 7

Reasoning: The cluster shows a high rate of HTTP 404 errors with consistent response times and no bytes transferred, indicating a potential flood attack targeting the authentication endpoint.
Common Pattern: The common behavior in this cluster is multiple POST requests to the /api/v1/auth/login endpoint resulting in HTTP 404 errors with similar response times and no data transferred.

[HTTP 500 Internal Server Error Flood] - Severity: High | Confidence: 0.90 | Logs: 9

Reasoning: The cluster shows a high rate of HTTP 500 errors with abnormal response times, indicating a potential flood attack targeting the server's resources.
Common Pattern: The common behavior in this cluster is multiple requests to different URLs resulting in HTTP 500 errors with high response times.

[HTTP 404 Error Flood] - Severity: High | Confidence: 0.80 | Logs: 14

Reasoning: The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.
Common Pattern: The common behavior in this cluster is multiple requests for specific URLs resulting in HTTP 404 errors with varying response times.

[HTTP 500 Internal Server Error] - Severity: High | Confidence: 0.90 | Logs: 7

Reasoning: The cluster shows a consistent pattern of HTTP 500 errors across multiple logs, indicating a potential server-side issue or misconfiguration.
Common Pattern: The common behavior in this cluster is the occurrence of HTTP 500 errors with high response times and no bytes transferred.

Anomaly Detection Report

Detailed Anomaly Logs

Anomaly #0 | Severity: High | Type: DoS (Score: 22970.0645)

Log Details:

```
syslog_ts: Jan 28 08:10:00 host: servernameabc process: httpd[12345] ip1: 10.141.146.187 ip2: 0.1.0.1 session_id: 75554 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:00 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 503 bytes: - response_time: 4366 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster of logs shows a high number of HTTP POST requests with a status of 503, indicating a potential denial of service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #195 | Severity: High | Type: DoS (Score: 22969.5938)

Log Details:

```
syslog_ts: Jan 28 08:12:22 host: servernameabc process: httpd[12345] ip1: 10.188.94.121 ip2: 0.1.0.1 session_id: 69665 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:22 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 503 bytes: - response_time: 3900 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster of logs shows a high number of HTTP POST requests with a status of 503, indicating a potential denial of service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #208 | Severity: High | Type: DoS (Score: 22966.6895)

Log Details:

```
syslog_ts: Jan 28 08:12:31 host: servernameabc process: httpd[12345] ip1: 10.228.193.77 ip2: 0.1.0.1 session_id: 17831 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:31 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 503 bytes: - response_time: 1869 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster of logs shows a high number of HTTP POST requests with a status of 503, indicating a potential denial of service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #403 | Severity: High | Type: DoS (Score: 22966.5371)

Log Details:

```
syslog_ts: Jan 28 08:14:50 host: servernameabc process: httpd[12345] ip1: 10.151.44.194 ip2: 0.1.0.1 session_id: 43599 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:50 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 503 bytes: - response_time: 1795 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster of logs shows a high number of HTTP POST requests with a status of 503, indicating a potential denial of service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #474 | Severity: High | Type: DoS (Score: 22969.3848)

Log Details:

```
syslog_ts: Jan 28 08:15:34 host: servernameabc process: httpd[12345] ip1: 10.130.196.185 ip2: 0.1.0.1 session_id: 55123 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:34 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 503 bytes: - response_time: 3707 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster of logs shows a high number of HTTP POST requests with a status of 503, indicating a potential denial of service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #504 | Severity: High | Type: DoS (Score: 22970.0645)

Log Details:

```
syslog_ts: Jan 28 08:15:56 host: servernameabc process: httpd[12345] ip1: 10.216.243.181 ip2: 0.1.0.1 session_id: 91935 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:56 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 503 bytes: - response_time: 4367 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster of logs shows a high number of HTTP POST requests with a status of 503, indicating a potential denial of service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #1 | Severity: High | Type: Data Exfiltration (Score: 19.6337)

Log Details:

```
syslog_ts: Jan 28 08:10:02 host: servernameabc process: httpd[12345] ip1: 10.148.114.112 ip2: 0.1.0.1 session_id: 47439 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:02 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 4261 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #5 | Severity: High | Type: Data Exfiltration (Score: 26.0371)

Log Details:

```
syslog_ts: Jan 28 08:10:05 host: servernameabc process: httpd[12345] ip1: 10.65.122.116 ip2: 0.1.0.1 session_id: 17753 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:05 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 14861 response_time: 26 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
```

like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #9 | Severity: High | Type: Data Exfiltration (Score: 24.2821)

Log Details:

syslog_ts: Jan 28 08:10:06 host: servernameabc process: httpd[12345] ip1: 10.191.145.44 ip2: 0.1.0.1 session_id: 44010 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:06 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 14116 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #13 | Severity: High | Type: Data Exfiltration (Score: 25.2601)

Log Details:

syslog_ts: Jan 28 08:10:09 host: servernameabc process: httpd[12345] ip1: 10.225.140.68 ip2: 0.1.0.1 session_id: 46330 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:09 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 16486 response_time: 10 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #16 | Severity: High | Type: Data Exfiltration (Score: 27.5933)

Log Details:

syslog_ts: Jan 28 08:10:11 host: servernameabc process: httpd[12345] ip1: 10.219.185.72 ip2: 0.1.0.1 session_id: 78164 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:11 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 18490 response_time: 35 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #18 | Severity: High | Type: Data Exfiltration (Score: 27.6903)

Log Details:

```
syslog_ts: Jan 28 08:10:13 host: servernameabc process: httpd[12345] ip1: 10.173.33.245 ip2: 0.1.0.1 session_id: 51120 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:13 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 17337 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #19 | Severity: High | Type: Data Exfiltration (Score: 20.4479)

Log Details:

```
syslog_ts: Jan 28 08:10:13 host: servernameabc process: httpd[12345] ip1: 10.43.58.51 ip2: 0.1.0.1 session_id: 31062 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:13 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 6097 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #20 | Severity: High | Type: Data Exfiltration (Score: 20.1544)

Log Details:

```
syslog_ts: Jan 28 08:10:14 host: servernameabc process: httpd[12345] ip1: 10.82.99.246 ip2: 0.1.0.1 session_id: 86464 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:14 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 5544 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #24 | Severity: High | Type: Data Exfiltration (Score: 23.7626)

Log Details:

```
syslog_ts: Jan 28 08:10:17 host: servernameabc process: httpd[12345] ip1: 10.57.247.144 ip2: 0.1.0.1 session_id: 30128 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:17 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 9672 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #28 | Severity: High | Type: Data Exfiltration (Score: 24.6881)

Log Details:

```
syslog_ts: Jan 28 08:10:20 host: servernameabc process: httpd[12345] ip1: 10.181.162.176 ip2: 0.1.0.1 session_id: 68796 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:20 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 14643 response_time: 10 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #31 | Severity: High | Type: Data Exfiltration (Score: 21.6715)

Log Details:

```
syslog_ts: Jan 28 08:10:22 host: servernameabc process: httpd[12345] ip1: 10.80.84.171 ip2: 0.1.0.1 session_id: 15422 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:22 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 7829 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #34 | Severity: High | Type: Data Exfiltration (Score: 27.1181)

Log Details:

```
syslog_ts: Jan 28 08:10:25 host: servernameabc process: httpd[12345] ip1: 10.55.139.142 ip2: 0.1.0.1 session_id: 51392 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:25 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 19561 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #35 | Severity: High | Type: Data Exfiltration (Score: 23.1411)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:10:25 host: servernameabc process: httpd[12345] ip1: 10.113.119.206 ip2: 0.1.0.1 session_id: 85530 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:25 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 7214 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #36 | Severity: High | Type: Data Exfiltration (Score: 26.2419)

Log Details:

```
syslog_ts: Jan 28 08:10:26 host: servernameabc process: httpd[12345] ip1: 10.120.221.62 ip2: 0.1.0.1 session_id: 72170 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:26 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 13060 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #39 | Severity: High | Type: Data Exfiltration (Score: 24.7113)

Log Details:

```
syslog_ts: Jan 28 08:10:28 host: servernameabc process: httpd[12345] ip1: 10.239.98.83 ip2: 0.1.0.1 session_id: 80264 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:28 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 9986 response_time: 36 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #42 | Severity: High | Type: Data Exfiltration (Score: 10.2831)

Log Details:

```
syslog_ts: Jan 28 08:10:30 host: servernameabc process: httpd[12345] ip1: 10.241.5.248 ip2: 0.1.0.1 session_id: 86438 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:30 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 213 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #46 | Severity: High | Type: Data Exfiltration (Score: 18.6340)

Log Details:

```
syslog_ts: Jan 28 08:10:34 host: servernameabc process: httpd[12345] ip1: 10.151.37.235 ip2: 0.1.0.1 session_id: 46620 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:34 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 2357 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #50 | Severity: High | Type: Data Exfiltration (Score: 20.0153)

Log Details:

```
syslog_ts: Jan 28 08:10:37 host: servernameabc process: httpd[12345] ip1: 10.248.85.140 ip2: 0.1.0.1 session_id: 45347 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:37 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 3462 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #51 | Severity: High | Type: Data Exfiltration (Score: 17.4754)

Log Details:

```
syslog_ts: Jan 28 08:10:38 host: servernameabc process: httpd[12345] ip1: 10.136.26.4 ip2: 0.1.0.1 session_id: 64172 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:38 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 2445 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #52 | Severity: High | Type: Data Exfiltration (Score: 23.2139)

Log Details:

```
syslog_ts: Jan 28 08:10:39 host: servernameabc process: httpd[12345] ip1: 10.76.109.182 ip2: 0.1.0.1 session_id: 12838 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:39 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 11565 response_time: 7 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #53 | Severity: High | Type: Data Exfiltration (Score: 23.5044)

Log Details:

syslog_ts: Jan 28 08:10:40 host: servernameabc process: httpd[12345] ip1: 10.32.7.137 ip2: 0.1.0.1 session_id: 88970 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:40 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 8105 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #55 | Severity: High | Type: Data Exfiltration (Score: 26.5748)

Log Details:

syslog_ts: Jan 28 08:10:40 host: servernameabc process: httpd[12345] ip1: 10.227.89.201 ip2: 0.1.0.1 session_id: 71136 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:40 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 17274 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #59 | Severity: High | Type: Data Exfiltration (Score: 24.6788)

Log Details:

syslog_ts: Jan 28 08:10:43 host: servernameabc process: httpd[12345] ip1: 10.24.238.70 ip2: 0.1.0.1 session_id: 85766 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:43 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 11301 response_time: 25 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #68 | Severity: High | Type: Data Exfiltration (Score: 25.3545)

Log Details:

```
syslog_ts: Jan 28 08:10:50 host: servernameabc process: httpd[12345] ip1: 10.230.222.174 ip2: 0.1.0.1 session_id: 17906 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:50 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 11980 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #69 | Severity: High | Type: Data Exfiltration (Score: 23.3067)

Log Details:

```
syslog_ts: Jan 28 08:10:50 host: servernameabc process: httpd[12345] ip1: 10.81.60.252 ip2: 0.1.0.1 session_id: 52157 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:50 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 6384 response_time: 50 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #70 | Severity: High | Type: Data Exfiltration (Score: 24.7960)

Log Details:

```
syslog_ts: Jan 28 08:10:51 host: servernameabc process: httpd[12345] ip1: 10.250.17.248 ip2: 0.1.0.1 session_id: 65893 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:51 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 13787 response_time: 14 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #71 | Severity: High | Type: Data Exfiltration (Score: 27.6275)

Log Details:

```
syslog_ts: Jan 28 08:10:52 host: servernameabc process: httpd[12345] ip1: 10.173.148.175 ip2: 0.1.0.1 session_id: 87550 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:52 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 19637 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #72 | Severity: High | Type: Data Exfiltration (Score: 23.8786)

```
Log Details:
syslog_ts: Jan 28 08:10:53 host: servernameabc process: httpd[12345] ip1: 10.225.68.250 ip2: 0.1.0.1
session_id: 80476 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:53 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 11817 response_time: 12 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #75 | Severity: High | Type: Data Exfiltration (Score: 26.5917)

```
Log Details:
syslog_ts: Jan 28 08:10:56 host: servernameabc process: httpd[12345] ip1: 10.31.194.118 ip2: 0.1.0.1
session_id: 16664 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:56 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 14321 response_time: 40 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #77 | Severity: High | Type: Data Exfiltration (Score: 20.8795)

```
Log Details:
syslog_ts: Jan 28 08:10:58 host: servernameabc process: httpd[12345] ip1: 10.89.32.173 ip2: 0.1.0.1
session_id: 87704 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:58 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 5955 response_time: 13 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #80 | Severity: High | Type: Data Exfiltration (Score: 24.1731)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:11:01 host: servernameabc process: httpd[12345] ip1: 10.131.134.3 ip2: 0.1.0.1
session_id: 32592 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:01 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 8433 response_time: 41 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #81 | Severity: High | Type: Data Exfiltration (Score: 12.9422)

```
Log Details:
syslog_ts: Jan 28 08:11:02 host: servernameabc process: httpd[12345] ip1: 10.245.60.247 ip2: 0.1.0.1
session_id: 99858 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:02 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 947 response_time: 6 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #85 | Severity: High | Type: Data Exfiltration (Score: 25.1493)

```
Log Details:
syslog_ts: Jan 28 08:11:04 host: servernameabc process: httpd[12345] ip1: 10.90.7.27 ip2: 0.1.0.1
session_id: 28934 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:04 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 15437 response_time: 12 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #88 | Severity: High | Type: Data Exfiltration (Score: 23.9865)

```
Log Details:
syslog_ts: Jan 28 08:11:06 host: servernameabc process: httpd[12345] ip1: 10.252.103.26 ip2: 0.1.0.1
session_id: 74140 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:06 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 8709 response_time: 34 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #89 | Severity: High | Type: Data Exfiltration (Score: 27.3303)

Log Details:

```
syslog_ts: Jan 28 08:11:06 host: servernameabc process: httpd[12345] ip1: 10.223.14.157 ip2: 0.1.0.1 session_id: 15418 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:06 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 18084 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #98 | Severity: High | Type: Data Exfiltration (Score: 20.4862)

Log Details:

```
syslog_ts: Jan 28 08:11:14 host: servernameabc process: httpd[12345] ip1: 10.141.209.201 ip2: 0.1.0.1 session_id: 76352 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:14 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 4522 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #103 | Severity: High | Type: Data Exfiltration (Score: 23.5764)

Log Details:

```
syslog_ts: Jan 28 08:11:17 host: servernameabc process: httpd[12345] ip1: 10.145.57.92 ip2: 0.1.0.1 session_id: 22132 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:17 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 7239 response_time: 43 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #104 | Severity: High | Type: Data Exfiltration (Score: 11.3797)

Log Details:

```
syslog_ts: Jan 28 08:11:18 host: servernameabc process: httpd[12345] ip1: 10.1.83.215 ip2: 0.1.0.1 session_id: 26408 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:18 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 408 response_time: 17 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #105 | Severity: High | Type: Data Exfiltration (Score: 25.5681)

Log Details:

syslog_ts: Jan 28 08:11:19 host: servernameabc process: httpd[12345] ip1: 10.161.61.182 ip2: 0.1.0.1 session_id: 46039 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:19 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 14220 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #108 | Severity: High | Type: Data Exfiltration (Score: 24.9261)

Log Details:

syslog_ts: Jan 28 08:11:20 host: servernameabc process: httpd[12345] ip1: 10.246.54.76 ip2: 0.1.0.1 session_id: 10747 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:20 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 10353 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #109 | Severity: High | Type: Data Exfiltration (Score: 22.6482)

Log Details:

syslog_ts: Jan 28 08:11:20 host: servernameabc process: httpd[12345] ip1: 10.181.172.75 ip2: 0.1.0.1 session_id: 35256 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:20 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 9710 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #113 | Severity: High | Type: Data Exfiltration (Score: 21.7282)

Log Details:

```
syslog_ts: Jan 28 08:11:22 host: servernameabc process: httpd[12345] ip1: 10.79.241.80 ip2: 0.1.0.1 session_id: 53687 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:22 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 4501 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #117 | Severity: High | Type: Data Exfiltration (Score: 23.6417)

Log Details:

```
syslog_ts: Jan 28 08:11:24 host: servernameabc process: httpd[12345] ip1: 10.92.81.166 ip2: 0.1.0.1 session_id: 47323 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:24 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 11479 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #124 | Severity: High | Type: Data Exfiltration (Score: 26.5671)

Log Details:

```
syslog_ts: Jan 28 08:11:28 host: servernameabc process: httpd[12345] ip1: 10.45.220.209 ip2: 0.1.0.1 session_id: 60991 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:28 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 13269 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #125 | Severity: High | Type: Data Exfiltration (Score: 23.0042)

Log Details:

```
syslog_ts: Jan 28 08:11:29 host: servernameabc process: httpd[12345] ip1: 10.162.115.220 ip2: 0.1.0.1 session_id: 86344 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:29 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 7526 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #126 | Severity: High | Type: Data Exfiltration (Score: 25.7737)

Log Details:

```
syslog_ts: Jan 28 08:11:29 host: servernameabc process: httpd[12345] ip1: 10.78.130.201 ip2: 0.1.0.1 session_id: 39591 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:29 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 13889 response_time: 27 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #129 | Severity: High | Type: Data Exfiltration (Score: 27.1325)

Log Details:

```
syslog_ts: Jan 28 08:11:32 host: servernameabc process: httpd[12345] ip1: 10.46.205.86 ip2: 0.1.0.1 session_id: 71726 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:32 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 15876 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #131 | Severity: High | Type: Data Exfiltration (Score: 19.4324)

Log Details:

```
syslog_ts: Jan 28 08:11:34 host: servernameabc process: httpd[12345] ip1: 10.179.131.93 ip2: 0.1.0.1 session_id: 70398 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:34 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 4240 response_time: 13 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #132 | Severity: High | Type: Data Exfiltration (Score: 27.0332)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:11:34 host: servernameabc process: httpd[12345] ip1: 10.163.202.149 ip2: 0.1.0.1
session_id: 92006 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:34 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 17017 response_time: 32 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #136 | Severity: High | Type: Data Exfiltration (Score: 24.3417)

Log Details:

```
syslog_ts: Jan 28 08:11:36 host: servernameabc process: httpd[12345] ip1: 10.208.30.213 ip2: 0.1.0.1
session_id: 66663 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:36 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 9021 response_time: 38 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #138 | Severity: High | Type: Data Exfiltration (Score: 27.0104)

Log Details:

```
syslog_ts: Jan 28 08:11:38 host: servernameabc process: httpd[12345] ip1: 10.111.148.173 ip2: 0.1.0.1
session_id: 15503 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:38 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 16580 response_time: 34 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #141 | Severity: High | Type: Data Exfiltration (Score: 26.3511)

Log Details:

```
syslog_ts: Jan 28 08:11:39 host: servernameabc process: httpd[12345] ip1: 10.129.154.222 ip2: 0.1.0.1
session_id: 95536 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:39 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 12572 response_time: 49 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #145 | Severity: High | Type: Data Exfiltration (Score: 22.6239)

Log Details:

```
syslog_ts: Jan 28 08:11:42 host: servernameabc process: httpd[12345] ip1: 10.52.196.239 ip2: 0.1.0.1 session_id: 13629 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:42 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 9911 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #146 | Severity: High | Type: Data Exfiltration (Score: 25.7818)

Log Details:

```
syslog_ts: Jan 28 08:11:42 host: servernameabc process: httpd[12345] ip1: 10.169.196.156 ip2: 0.1.0.1 session_id: 74043 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:42 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 14273 response_time: 25 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #147 | Severity: High | Type: Data Exfiltration (Score: 27.2823)

Log Details:

```
syslog_ts: Jan 28 08:11:43 host: servernameabc process: httpd[12345] ip1: 10.132.136.210 ip2: 0.1.0.1 session_id: 53231 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:43 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 17717 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #151 | Severity: High | Type: Data Exfiltration (Score: 20.8208)

Log Details:

```
syslog_ts: Jan 28 08:11:47 host: servernameabc process: httpd[12345] ip1: 10.100.192.246 ip2: 0.1.0.1 session_id: 56433 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:47 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 4016 response_time: 38 referer:
```

```
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #153 | Severity: High | Type: Data Exfiltration (Score: 17.0479)

Log Details:

```
syslog_ts: Jan 28 08:11:49  host: servernameabc  process: httpd[12345]  ip1: 10.54.64.43  ip2: 0.1.0.1  session_id: 70910  domain: abc.example.net  apache_ts: 28/Jan/2026:08:11:49 +0530  request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1  status: 200  bytes: 1707  response_time: 30  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #155 | Severity: High | Type: Data Exfiltration (Score: 22.9399)

Log Details:

```
syslog_ts: Jan 28 08:11:51  host: servernameabc  process: httpd[12345]  ip1: 10.249.3.109  ip2: 0.1.0.1  session_id: 79284  domain: abc.example.net  apache_ts: 28/Jan/2026:08:11:51 +0530  request: POST /api/v1/auth/login HTTP/1.1  status: 200  bytes: 6392  response_time: 41  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #159 | Severity: High | Type: Data Exfiltration (Score: 22.0037)

Log Details:

```
syslog_ts: Jan 28 08:11:54  host: servernameabc  process: httpd[12345]  ip1: 10.16.188.139  ip2: 0.1.0.1  session_id: 70087  domain: abc.example.net  apache_ts: 28/Jan/2026:08:11:54 +0530  request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1  status: 200  bytes: 5375  response_time: 37  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #160 | Severity: High | Type: Data Exfiltration (Score: 27.2369)

Log Details:

```
syslog_ts: Jan 28 08:11:55 host: servernameabc process: httpd[12345] ip1: 10.181.134.121 ip2: 0.1.0.1 session_id: 76923 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:55 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 15140 response_time: 49 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #167 | Severity: High | Type: Data Exfiltration (Score: 26.3560)

Log Details:

```
syslog_ts: Jan 28 08:12:02 host: servernameabc process: httpd[12345] ip1: 10.37.123.178 ip2: 0.1.0.1 session_id: 48588 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:02 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 14036 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #168 | Severity: High | Type: Data Exfiltration (Score: 23.5839)

Log Details:

```
syslog_ts: Jan 28 08:12:03 host: servernameabc process: httpd[12345] ip1: 10.217.111.39 ip2: 0.1.0.1 session_id: 99187 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:03 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 7626 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #170 | Severity: High | Type: Data Exfiltration (Score: 16.2904)

Log Details:

```
syslog_ts: Jan 28 08:12:05 host: servernameabc process: httpd[12345] ip1: 10.238.69.65 ip2: 0.1.0.1 session_id: 70377 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:05 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 1974 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #171 | Severity: High | Type: Data Exfiltration (Score: 26.8677)

Log Details:

```
syslog_ts: Jan 28 08:12:05 host: servernameabc process: httpd[12345] ip1: 10.117.147.45 ip2: 0.1.0.1 session_id: 46800 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:05 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 19720 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #173 | Severity: High | Type: Data Exfiltration (Score: 26.8134)

Log Details:

```
syslog_ts: Jan 28 08:12:08 host: servernameabc process: httpd[12345] ip1: 10.200.65.5 ip2: 0.1.0.1 session_id: 49265 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:08 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 17024 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #175 | Severity: High | Type: Data Exfiltration (Score: 28.5265)

Log Details:

```
syslog_ts: Jan 28 08:12:08 host: servernameabc process: httpd[12345] ip1: 10.174.203.195 ip2: 0.1.0.1 session_id: 67399 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:08 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 19879 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #178 | Severity: High | Type: Data Exfiltration (Score: 27.1676)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:12:10 host: servernameabc process: httpd[12345] ip1: 10.243.38.239 ip2: 0.1.0.1 session_id: 93985 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:10 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 18303 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #179 | Severity: High | Type: Data Exfiltration (Score: 26.1435)

Log Details:

```
syslog_ts: Jan 28 08:12:11 host: servernameabc process: httpd[12345] ip1: 10.186.144.229 ip2: 0.1.0.1 session_id: 58069 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:11 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 19323 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #182 | Severity: High | Type: Data Exfiltration (Score: 22.6857)

Log Details:

```
syslog_ts: Jan 28 08:12:13 host: servernameabc process: httpd[12345] ip1: 10.91.217.194 ip2: 0.1.0.1 session_id: 35872 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:13 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 8430 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #184 | Severity: High | Type: Data Exfiltration (Score: 16.8085)

Log Details:

```
syslog_ts: Jan 28 08:12:14 host: servernameabc process: httpd[12345] ip1: 10.237.227.85 ip2: 0.1.0.1 session_id: 70966 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:14 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 1895 response_time: 20 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #186 | Severity: High | Type: Data Exfiltration (Score: 19.8866)

Log Details:

```
syslog_ts: Jan 28 08:12:15 host: servernameabc process: httpd[12345] ip1: 10.40.90.251 ip2: 0.1.0.1 session_id: 13936 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:15 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 2870 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #187 | Severity: High | Type: Data Exfiltration (Score: 15.1015)

Log Details:

```
syslog_ts: Jan 28 08:12:16 host: servernameabc process: httpd[12345] ip1: 10.53.173.166 ip2: 0.1.0.1 session_id: 34616 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:16 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 1615 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #191 | Severity: High | Type: Data Exfiltration (Score: 17.6471)

Log Details:

```
syslog_ts: Jan 28 08:12:20 host: servernameabc process: httpd[12345] ip1: 10.250.232.174 ip2: 0.1.0.1 session_id: 88397 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:20 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 1692 response_time: 43 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #192 | Severity: High | Type: Data Exfiltration (Score: 25.2206)

Log Details:

```
syslog_ts: Jan 28 08:12:20 host: servernameabc process: httpd[12345] ip1: 10.235.129.48 ip2: 0.1.0.1 session_id: 99485 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:20 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 10308 response_time: 44 referer:
```

```
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #196 | Severity: High | Type: Data Exfiltration (Score: 25.4842)

```
Log Details:
syslog_ts: Jan 28 08:12:24  host: servernameabc  process: httpd[12345]  ip1: 10.181.215.119  ip2: 0.1.0.1  session_id: 84831  domain: abc.example.net  apache_ts: 28/Jan/2026:08:12:24 +0530  request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1  status: 200  bytes: 17263  response_time: 10  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #199 | Severity: High | Type: Data Exfiltration (Score: 22.3865)

```
Log Details:
syslog_ts: Jan 28 08:12:24  host: servernameabc  process: httpd[12345]  ip1: 10.253.56.103  ip2: 0.1.0.1  session_id: 40327  domain: abc.example.net  apache_ts: 28/Jan/2026:08:12:24 +0530  request: POST /leaverest/rest/lwpBatch HTTP/1.1  status: 200  bytes: 5571  response_time: 42  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #203 | Severity: High | Type: Data Exfiltration (Score: 20.6220)

```
Log Details:
syslog_ts: Jan 28 08:12:28  host: servernameabc  process: httpd[12345]  ip1: 10.20.162.208  ip2: 0.1.0.1  session_id: 78010  domain: abc.example.net  apache_ts: 28/Jan/2026:08:12:28 +0530  request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1  status: 200  bytes: 4114  response_time: 32  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #205 | Severity: High | Type: Data Exfiltration (Score: 25.8081)

Log Details:

```
syslog_ts: Jan 28 08:12:30 host: servernameabc process: httpd[12345] ip1: 10.30.197.40 ip2: 0.1.0.1 session_id: 15252 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:30 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 15167 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #207 | Severity: High | Type: Data Exfiltration (Score: 27.4808)

Log Details:

```
syslog_ts: Jan 28 08:12:31 host: servernameabc process: httpd[12345] ip1: 10.37.106.97 ip2: 0.1.0.1 session_id: 74587 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:31 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 19062 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #211 | Severity: High | Type: Data Exfiltration (Score: 26.6118)

Log Details:

```
syslog_ts: Jan 28 08:12:32 host: servernameabc process: httpd[12345] ip1: 10.240.111.166 ip2: 0.1.0.1 session_id: 34169 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:32 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 14247 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #213 | Severity: High | Type: Data Exfiltration (Score: 14.8917)

Log Details:

```
syslog_ts: Jan 28 08:12:33 host: servernameabc process: httpd[12345] ip1: 10.42.224.71 ip2: 0.1.0.1 session_id: 66068 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:33 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 827 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #220 | Severity: High | Type: Data Exfiltration (Score: 27.1814)

Log Details:

```
syslog_ts: Jan 28 08:12:40 host: servernameabc process: httpd[12345] ip1: 10.10.107.181 ip2: 0.1.0.1 session_id: 92721 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:40 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 17542 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #223 | Severity: High | Type: Data Exfiltration (Score: 21.9336)

Log Details:

```
syslog_ts: Jan 28 08:12:42 host: servernameabc process: httpd[12345] ip1: 10.58.221.131 ip2: 0.1.0.1 session_id: 31573 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:42 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 5173 response_time: 39 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #225 | Severity: High | Type: Data Exfiltration (Score: 21.7868)

Log Details:

```
syslog_ts: Jan 28 08:12:43 host: servernameabc process: httpd[12345] ip1: 10.77.75.128 ip2: 0.1.0.1 session_id: 45959 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:43 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 4698 response_time: 45 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #227 | Severity: High | Type: Data Exfiltration (Score: 26.2382)

Log Details:

```
syslog_ts: Jan 28 08:12:44 host: servernameabc process: httpd[12345] ip1: 10.43.226.187 ip2: 0.1.0.1
session_id: 79863 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:44 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 12483 response_time: 47 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #229 | Severity: High | Type: Data Exfiltration (Score: 16.0408)

Log Details:

```
syslog_ts: Jan 28 08:12:46 host: servernameabc process: httpd[12345] ip1: 10.10.227.7 ip2: 0.1.0.1
session_id: 52548 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:46 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 1757 response_time: 14 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #231 | Severity: High | Type: Data Exfiltration (Score: 20.9953)

Log Details:

```
syslog_ts: Jan 28 08:12:48 host: servernameabc process: httpd[12345] ip1: 10.145.217.30 ip2: 0.1.0.1
session_id: 16382 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:48 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 3811 response_time: 47 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #234 | Severity: High | Type: Data Exfiltration (Score: 26.1774)

Log Details:

```
syslog_ts: Jan 28 08:12:49 host: servernameabc process: httpd[12345] ip1: 10.133.176.141 ip2: 0.1.0.1
session_id: 19649 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:49 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 18692 response_time: 13 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #236 | Severity: High | Type: Data Exfiltration (Score: 26.0221)

Log Details:

```
syslog_ts: Jan 28 08:12:50 host: servernameabc process: httpd[12345] ip1: 10.233.142.136 ip2: 0.1.0.1 session_id: 81047 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:50 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 18110 response_time: 13 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #237 | Severity: High | Type: Data Exfiltration (Score: 20.6764)

Log Details:

```
syslog_ts: Jan 28 08:12:51 host: servernameabc process: httpd[12345] ip1: 10.160.64.223 ip2: 0.1.0.1 session_id: 71561 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:51 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 3526 response_time: 47 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #240 | Severity: High | Type: Data Exfiltration (Score: 22.5290)

Log Details:

```
syslog_ts: Jan 28 08:12:53 host: servernameabc process: httpd[12345] ip1: 10.161.230.131 ip2: 0.1.0.1 session_id: 84421 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:53 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 9019 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #246 | Severity: High | Type: Data Exfiltration (Score: 27.2782)

Log Details:

```
syslog_ts: Jan 28 08:12:56 host: servernameabc process: httpd[12345] ip1: 10.253.160.235 ip2: 0.1.0.1 session_id: 75289 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:56 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 16513 response_time: 40 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #253 | Severity: High | Type: Data Exfiltration (Score: 23.2581)

Log Details:

syslog_ts: Jan 28 08:13:01 host: servernameabc process: httpd[12345] ip1: 10.228.202.53 ip2: 0.1.0.1 session_id: 22399 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:01 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 8659 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #255 | Severity: High | Type: Data Exfiltration (Score: 26.3137)

Log Details:

syslog_ts: Jan 28 08:13:02 host: servernameabc process: httpd[12345] ip1: 10.173.61.97 ip2: 0.1.0.1 session_id: 54454 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:02 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 13912 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #257 | Severity: High | Type: Data Exfiltration (Score: 21.0451)

Log Details:

syslog_ts: Jan 28 08:13:03 host: servernameabc process: httpd[12345] ip1: 10.200.252.25 ip2: 0.1.0.1 session_id: 55428 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:03 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 7650 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #259 | Severity: High | Type: Data Exfiltration (Score: 16.0689)

Log Details:

```
syslog_ts: Jan 28 08:13:04 host: servernameabc process: httpd[12345] ip1: 10.20.26.46 ip2: 0.1.0.1 session_id: 64566 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:04 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 2321 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #260 | Severity: High | Type: Data Exfiltration (Score: 25.1244)

Log Details:

```
syslog_ts: Jan 28 08:13:04 host: servernameabc process: httpd[12345] ip1: 10.181.191.100 ip2: 0.1.0.1 session_id: 61393 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:04 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 11537 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #262 | Severity: High | Type: Data Exfiltration (Score: 20.2816)

Log Details:

```
syslog_ts: Jan 28 08:13:06 host: servernameabc process: httpd[12345] ip1: 10.83.169.52 ip2: 0.1.0.1 session_id: 73617 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:06 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 3444 response_time: 40 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #267 | Severity: High | Type: Data Exfiltration (Score: 28.2230)

Log Details:

```
syslog_ts: Jan 28 08:13:10 host: servernameabc process: httpd[12345] ip1: 10.147.69.89 ip2: 0.1.0.1 session_id: 28076 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:10 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 19325 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #271 | Severity: High | Type: Data Exfiltration (Score: 23.0695)

Log Details:

```
syslog_ts: Jan 28 08:13:12 host: servernameabc process: httpd[12345] ip1: 10.79.51.54 ip2: 0.1.0.1 session_id: 89071 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:12 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 11213 response_time: 7 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #272 | Severity: High | Type: Data Exfiltration (Score: 25.0812)

Log Details:

```
syslog_ts: Jan 28 08:13:14 host: servernameabc process: httpd[12345] ip1: 10.17.236.35 ip2: 0.1.0.1 session_id: 38491 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:14 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 14367 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #275 | Severity: High | Type: Data Exfiltration (Score: 26.1113)

Log Details:

```
syslog_ts: Jan 28 08:13:15 host: servernameabc process: httpd[12345] ip1: 10.30.168.15 ip2: 0.1.0.1 session_id: 68160 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:15 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 19615 response_time: 10 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #279 | Severity: High | Type: Data Exfiltration (Score: 27.8236)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:13:17 host: servernameabc process: httpd[12345] ip1: 10.229.120.174 ip2: 0.1.0.1 session_id: 30744 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:17 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 19574 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #282 | Severity: High | Type: Data Exfiltration (Score: 17.0215)

Log Details:

```
syslog_ts: Jan 28 08:13:18 host: servernameabc process: httpd[12345] ip1: 10.30.9.4 ip2: 0.1.0.1 session_id: 76757 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:18 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 2223 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #283 | Severity: High | Type: Data Exfiltration (Score: 26.0879)

Log Details:

```
syslog_ts: Jan 28 08:13:20 host: servernameabc process: httpd[12345] ip1: 10.231.73.90 ip2: 0.1.0.1 session_id: 48062 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:20 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 13403 response_time: 36 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #286 | Severity: High | Type: Data Exfiltration (Score: 24.4521)

Log Details:

```
syslog_ts: Jan 28 08:13:21 host: servernameabc process: httpd[12345] ip1: 10.232.75.133 ip2: 0.1.0.1 session_id: 92422 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:21 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 12361 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #289 | Severity: High | Type: Data Exfiltration (Score: 25.4570)

Log Details:

```
syslog_ts: Jan 28 08:13:24 host: servernameabc process: httpd[12345] ip1: 10.237.149.233 ip2: 0.1.0.1 session_id: 46481 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:24 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 14308 response_time: 20 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #290 | Severity: High | Type: Data Exfiltration (Score: 22.5028)

Log Details:

```
syslog_ts: Jan 28 08:13:25 host: servernameabc process: httpd[12345] ip1: 10.5.246.227 ip2: 0.1.0.1 session_id: 68275 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:25 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 7949 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #291 | Severity: High | Type: Data Exfiltration (Score: 25.8115)

Log Details:

```
syslog_ts: Jan 28 08:13:25 host: servernameabc process: httpd[12345] ip1: 10.176.212.74 ip2: 0.1.0.1 session_id: 55323 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:25 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 15641 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #295 | Severity: High | Type: Data Exfiltration (Score: 22.3633)

Log Details:

```
syslog_ts: Jan 28 08:13:29 host: servernameabc process: httpd[12345] ip1: 10.222.155.6 ip2: 0.1.0.1 session_id: 19643 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:29 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 6190 response_time: 32 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #303 | Severity: High | Type: Data Exfiltration (Score: 19.8301)

Log Details:

syslog_ts: Jan 28 08:13:34 host: servernameabc process: httpd[12345] ip1: 10.137.27.156 ip2: 0.1.0.1 session_id: 99386 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:34 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 4376 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #304 | Severity: High | Type: Data Exfiltration (Score: 21.7540)

Log Details:

syslog_ts: Jan 28 08:13:35 host: servernameabc process: httpd[12345] ip1: 10.74.35.187 ip2: 0.1.0.1 session_id: 96685 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:35 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 6598 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #308 | Severity: High | Type: Data Exfiltration (Score: 27.2004)

Log Details:

syslog_ts: Jan 28 08:13:39 host: servernameabc process: httpd[12345] ip1: 10.86.170.223 ip2: 0.1.0.1 session_id: 18588 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:39 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 16562 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #310 | Severity: High | Type: Data Exfiltration (Score: 13.2550)

Log Details:

```
syslog_ts: Jan 28 08:13:39 host: servernameabc process: httpd[12345] ip1: 10.170.130.236 ip2: 0.1.0.1 session_id: 76025 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:39 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 740 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #312 | Severity: High | Type: Data Exfiltration (Score: 25.4959)

Log Details:

```
syslog_ts: Jan 28 08:13:41 host: servernameabc process: httpd[12345] ip1: 10.184.34.202 ip2: 0.1.0.1 session_id: 74864 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:41 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 13811 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #318 | Severity: High | Type: Data Exfiltration (Score: 26.0440)

Log Details:

```
syslog_ts: Jan 28 08:13:47 host: servernameabc process: httpd[12345] ip1: 10.237.220.118 ip2: 0.1.0.1 session_id: 20315 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:47 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 12763 response_time: 40 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #320 | Severity: High | Type: Data Exfiltration (Score: 25.6073)

Log Details:

```
syslog_ts: Jan 28 08:13:48 host: servernameabc process: httpd[12345] ip1: 10.234.194.176 ip2: 0.1.0.1 session_id: 81033 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:48 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 11983 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #326 | Severity: High | Type: Data Exfiltration (Score: 27.3627)

Log Details:

```
syslog_ts: Jan 28 08:13:54 host: servernameabc process: httpd[12345] ip1: 10.153.89.252 ip2: 0.1.0.1 session_id: 94044 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:54 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 16961 response_time: 39 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #333 | Severity: High | Type: Data Exfiltration (Score: 22.2996)

Log Details:

```
syslog_ts: Jan 28 08:13:59 host: servernameabc process: httpd[12345] ip1: 10.127.8.94 ip2: 0.1.0.1 session_id: 48215 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:59 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 6991 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #337 | Severity: High | Type: Data Exfiltration (Score: 18.5741)

Log Details:

```
syslog_ts: Jan 28 08:14:01 host: servernameabc process: httpd[12345] ip1: 10.222.215.40 ip2: 0.1.0.1 session_id: 31435 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:01 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 2620 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #338 | Severity: High | Type: Data Exfiltration (Score: 26.1537)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:14:02 host: servernameabc process: httpd[12345] ip1: 10.50.76.33 ip2: 0.1.0.1 session_id: 80298 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:02 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 18256 response_time: 14 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #345 | Severity: High | Type: Data Exfiltration (Score: 15.7563)

Log Details:

```
syslog_ts: Jan 28 08:14:06 host: servernameabc process: httpd[12345] ip1: 10.1.206.221 ip2: 0.1.0.1 session_id: 83539 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:06 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 1215 response_time: 29 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #347 | Severity: High | Type: Data Exfiltration (Score: 23.6730)

Log Details:

```
syslog_ts: Jan 28 08:14:09 host: servernameabc process: httpd[12345] ip1: 10.85.185.162 ip2: 0.1.0.1 session_id: 11502 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:09 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 9629 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #349 | Severity: High | Type: Data Exfiltration (Score: 23.0360)

Log Details:

```
syslog_ts: Jan 28 08:14:11 host: servernameabc process: httpd[12345] ip1: 10.209.4.196 ip2: 0.1.0.1 session_id: 23452 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:11 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 8244 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #352 | Severity: High | Type: Data Exfiltration (Score: 14.9122)

Log Details:

```
syslog_ts: Jan 28 08:14:15 host: servernameabc process: httpd[12345] ip1: 10.145.249.4 ip2: 0.1.0.1 session_id: 36893 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:15 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 749 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #354 | Severity: High | Type: Data Exfiltration (Score: 26.4907)

Log Details:

```
syslog_ts: Jan 28 08:14:16 host: servernameabc process: httpd[12345] ip1: 10.223.138.98 ip2: 0.1.0.1 session_id: 46048 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:16 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 17460 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #357 | Severity: High | Type: Data Exfiltration (Score: 24.6786)

Log Details:

```
syslog_ts: Jan 28 08:14:18 host: servernameabc process: httpd[12345] ip1: 10.167.36.240 ip2: 0.1.0.1 session_id: 17760 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:18 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 12535 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #360 | Severity: High | Type: Data Exfiltration (Score: 28.2791)

Log Details:

```
syslog_ts: Jan 28 08:14:20 host: servernameabc process: httpd[12345] ip1: 10.135.48.18 ip2: 0.1.0.1 session_id: 45456 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:20 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 19889 response_time: 42 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #363 | Severity: High | Type: Data Exfiltration (Score: 20.2609)

Log Details:

syslog_ts: Jan 28 08:14:22 host: servernameabc process: httpd[12345] ip1: 10.163.49.220 ip2: 0.1.0.1 session_id: 56962 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:22 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 3215 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #364 | Severity: High | Type: Data Exfiltration (Score: 24.2666)

Log Details:

syslog_ts: Jan 28 08:14:23 host: servernameabc process: httpd[12345] ip1: 10.168.109.57 ip2: 0.1.0.1 session_id: 36576 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:23 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 9586 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #365 | Severity: High | Type: Data Exfiltration (Score: 26.4268)

Log Details:

syslog_ts: Jan 28 08:14:25 host: servernameabc process: httpd[12345] ip1: 10.45.101.140 ip2: 0.1.0.1 session_id: 60236 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:25 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 18955 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #366 | Severity: High | Type: Data Exfiltration (Score: 20.0372)

Log Details:

```
syslog_ts: Jan 28 08:14:26 host: servernameabc process: httpd[12345] ip1: 10.51.143.178 ip2: 0.1.0.1 session_id: 79348 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:26 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 4597 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #367 | Severity: High | Type: Data Exfiltration (Score: 19.5373)

Log Details:

```
syslog_ts: Jan 28 08:14:27 host: servernameabc process: httpd[12345] ip1: 10.132.205.118 ip2: 0.1.0.1 session_id: 28263 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:27 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 5424 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #371 | Severity: High | Type: Data Exfiltration (Score: 27.3161)

Log Details:

```
syslog_ts: Jan 28 08:14:29 host: servernameabc process: httpd[12345] ip1: 10.195.242.157 ip2: 0.1.0.1 session_id: 89614 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:29 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 16340 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #373 | Severity: High | Type: Data Exfiltration (Score: 24.2985)

Log Details:

```
syslog_ts: Jan 28 08:14:30 host: servernameabc process: httpd[12345] ip1: 10.232.186.17 ip2: 0.1.0.1 session_id: 17786 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:30 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 10141 response_time: 27 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #382 | Severity: High | Type: Data Exfiltration (Score: 24.6246)

Log Details:

```
syslog_ts: Jan 28 08:14:36 host: servernameabc process: httpd[12345] ip1: 10.162.232.47 ip2: 0.1.0.1 session_id: 57432 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:36 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 14792 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #384 | Severity: High | Type: Data Exfiltration (Score: 23.0620)

Log Details:

```
syslog_ts: Jan 28 08:14:36 host: servernameabc process: httpd[12345] ip1: 10.185.111.253 ip2: 0.1.0.1 session_id: 70802 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:36 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 6036 response_time: 50 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #387 | Severity: High | Type: Data Exfiltration (Score: 24.7325)

Log Details:

```
syslog_ts: Jan 28 08:14:40 host: servernameabc process: httpd[12345] ip1: 10.158.116.102 ip2: 0.1.0.1 session_id: 84655 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:40 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 10251 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #389 | Severity: High | Type: Data Exfiltration (Score: 18.3563)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:14:42 host: servernameabc process: httpd[12345] ip1: 10.212.121.132 ip2: 0.1.0.1
session_id: 65236 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:42 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 2516 response_time: 27 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #396 | Severity: High | Type: Data Exfiltration (Score: 22.6158)

```
Log Details:
syslog_ts: Jan 28 08:14:46 host: servernameabc process: httpd[12345] ip1: 10.212.212.19 ip2: 0.1.0.1
session_id: 47014 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:46 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 5649 response_time: 46 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #399 | Severity: High | Type: Data Exfiltration (Score: 16.3564)

```
Log Details:
syslog_ts: Jan 28 08:14:48 host: servernameabc process: httpd[12345] ip1: 10.17.37.110 ip2: 0.1.0.1
session_id: 13090 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:48 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 1414 response_time: 30 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #400 | Severity: High | Type: Data Exfiltration (Score: 23.8170)

```
Log Details:
syslog_ts: Jan 28 08:14:48 host: servernameabc process: httpd[12345] ip1: 10.230.23.199 ip2: 0.1.0.1
session_id: 15821 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:48 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 7715 response_time: 42 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #401 | Severity: High | Type: Data Exfiltration (Score: 16.0043)

Log Details:

```
syslog_ts: Jan 28 08:14:49 host: servernameabc process: httpd[12345] ip1: 10.66.248.34 ip2: 0.1.0.1 session_id: 28095 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:49 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 1034 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #402 | Severity: High | Type: Data Exfiltration (Score: 25.6461)

Log Details:

```
syslog_ts: Jan 28 08:14:49 host: servernameabc process: httpd[12345] ip1: 10.137.200.84 ip2: 0.1.0.1 session_id: 22942 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:49 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 16155 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #405 | Severity: High | Type: Data Exfiltration (Score: 21.9889)

Log Details:

```
syslog_ts: Jan 28 08:14:52 host: servernameabc process: httpd[12345] ip1: 10.86.183.116 ip2: 0.1.0.1 session_id: 42321 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:52 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 5417 response_time: 36 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #406 | Severity: High | Type: Data Exfiltration (Score: 24.8414)

Log Details:

```
syslog_ts: Jan 28 08:14:52 host: servernameabc process: httpd[12345] ip1: 10.10.113.13 ip2: 0.1.0.1 session_id: 76944 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:52 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 15118 response_time: 10 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #409 | Severity: High | Type: Data Exfiltration (Score: 21.7054)

Log Details:

syslog_ts: Jan 28 08:14:54 host: servernameabc process: httpd[12345] ip1: 10.153.83.220 ip2: 0.1.0.1 session_id: 98410 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:54 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 4750 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #412 | Severity: High | Type: Data Exfiltration (Score: 24.8834)

Log Details:

syslog_ts: Jan 28 08:14:55 host: servernameabc process: httpd[12345] ip1: 10.48.13.53 ip2: 0.1.0.1 session_id: 93931 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:55 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 9669 response_time: 43 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #421 | Severity: High | Type: Data Exfiltration (Score: 25.6077)

Log Details:

syslog_ts: Jan 28 08:15:02 host: servernameabc process: httpd[12345] ip1: 10.76.65.14 ip2: 0.1.0.1 session_id: 26491 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:02 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 12108 response_time: 36 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #424 | Severity: High | Type: Data Exfiltration (Score: 25.9551)

Log Details:

```
syslog_ts: Jan 28 08:15:03 host: servernameabc process: httpd[12345] ip1: 10.124.154.220 ip2: 0.1.0.1 session_id: 92490 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:03 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 15869 response_time: 20 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #429 | Severity: High | Type: Data Exfiltration (Score: 24.9508)

Log Details:

```
syslog_ts: Jan 28 08:15:06 host: servernameabc process: httpd[12345] ip1: 10.206.73.15 ip2: 0.1.0.1 session_id: 92804 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:06 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 13277 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #431 | Severity: High | Type: Data Exfiltration (Score: 24.0980)

Log Details:

```
syslog_ts: Jan 28 08:15:06 host: servernameabc process: httpd[12345] ip1: 10.243.35.177 ip2: 0.1.0.1 session_id: 66724 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:06 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 8462 response_time: 39 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #434 | Severity: High | Type: Data Exfiltration (Score: 27.1336)

Log Details:

```
syslog_ts: Jan 28 08:15:09 host: servernameabc process: httpd[12345] ip1: 10.228.247.178 ip2: 0.1.0.1 session_id: 52077 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:09 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 15065 response_time: 47 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #435 | Severity: High | Type: Data Exfiltration (Score: 26.8629)

```
Log Details:
syslog_ts: Jan 28 08:15:10 host: servernameabc process: httpd[12345] ip1: 10.226.110.8 ip2: 0.1.0.1 session_id: 30354 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:10 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 15599 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #436 | Severity: High | Type: Data Exfiltration (Score: 21.0400)

```
Log Details:
syslog_ts: Jan 28 08:15:10 host: servernameabc process: httpd[12345] ip1: 10.98.87.4 ip2: 0.1.0.1 session_id: 35746 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:10 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 6622 response_time: 10 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #438 | Severity: High | Type: Data Exfiltration (Score: 21.1310)

```
Log Details:
syslog_ts: Jan 28 08:15:12 host: servernameabc process: httpd[12345] ip1: 10.135.170.67 ip2: 0.1.0.1 session_id: 21859 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:12 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 6934 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #447 | Severity: High | Type: Data Exfiltration (Score: 18.9642)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:15:18 host: servernameabc process: httpd[12345] ip1: 10.156.47.100 ip2: 0.1.0.1
session_id: 30478 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:18 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 4583 response_time: 6 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #454 | Severity: High | Type: Data Exfiltration (Score: 19.0031)

```
Log Details:
syslog_ts: Jan 28 08:15:21 host: servernameabc process: httpd[12345] ip1: 10.60.114.183 ip2: 0.1.0.1
session_id: 27979 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:21 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 2500 response_time: 40 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #456 | Severity: High | Type: Data Exfiltration (Score: 27.2296)

```
Log Details:
syslog_ts: Jan 28 08:15:21 host: servernameabc process: httpd[12345] ip1: 10.226.95.5 ip2: 0.1.0.1
session_id: 49320 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:21 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 16051 response_time: 42 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #460 | Severity: High | Type: Data Exfiltration (Score: 20.6580)

```
Log Details:
syslog_ts: Jan 28 08:15:25 host: servernameabc process: httpd[12345] ip1: 10.118.14.151 ip2: 0.1.0.1
session_id: 41418 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:25 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 4376 response_time: 28 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #462 | Severity: High | Type: Data Exfiltration (Score: 23.6138)

Log Details:

```
syslog_ts: Jan 28 08:15:26 host: servernameabc process: httpd[12345] ip1: 10.165.105.59 ip2: 0.1.0.1 session_id: 27384 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:26 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 8848 response_time: 26 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #466 | Severity: High | Type: Data Exfiltration (Score: 25.4265)

Log Details:

```
syslog_ts: Jan 28 08:15:28 host: servernameabc process: httpd[12345] ip1: 10.76.226.155 ip2: 0.1.0.1 session_id: 50841 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:28 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 10402 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #467 | Severity: High | Type: Data Exfiltration (Score: 20.1615)

Log Details:

```
syslog_ts: Jan 28 08:15:29 host: servernameabc process: httpd[12345] ip1: 10.227.103.233 ip2: 0.1.0.1 session_id: 68888 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:29 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 3169 response_time: 45 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #470 | Severity: High | Type: Data Exfiltration (Score: 26.1330)

Log Details:

```
syslog_ts: Jan 28 08:15:31 host: servernameabc process: httpd[12345] ip1: 10.112.208.119 ip2: 0.1.0.1 session_id: 60545 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:31 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 18524 response_time: 13 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #475 | Severity: High | Type: Data Exfiltration (Score: 25.8613)

Log Details:

syslog_ts: Jan 28 08:15:35 host: servernameabc process: httpd[12345] ip1: 10.7.14.50 ip2: 0.1.0.1 session_id: 69151 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:35 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 11326 response_time: 49 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #479 | Severity: High | Type: Data Exfiltration (Score: 25.0212)

Log Details:

syslog_ts: Jan 28 08:15:38 host: servernameabc process: httpd[12345] ip1: 10.20.130.237 ip2: 0.1.0.1 session_id: 40216 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:38 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 15032 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #480 | Severity: High | Type: Data Exfiltration (Score: 20.8568)

Log Details:

syslog_ts: Jan 28 08:15:39 host: servernameabc process: httpd[12345] ip1: 10.109.97.164 ip2: 0.1.0.1 session_id: 30309 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:39 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 4051 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #485 | Severity: High | Type: Data Exfiltration (Score: 26.4404)

Log Details:

```
syslog_ts: Jan 28 08:15:45 host: servernameabc process: httpd[12345] ip1: 10.195.157.82 ip2: 0.1.0.1 session_id: 38344 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:45 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 17281 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #487 | Severity: High | Type: Data Exfiltration (Score: 25.3356)

Log Details:

```
syslog_ts: Jan 28 08:15:46 host: servernameabc process: httpd[12345] ip1: 10.180.29.189 ip2: 0.1.0.1 session_id: 26378 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:46 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 16044 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #488 | Severity: High | Type: Data Exfiltration (Score: 23.7546)

Log Details:

```
syslog_ts: Jan 28 08:15:47 host: servernameabc process: httpd[12345] ip1: 10.130.62.32 ip2: 0.1.0.1 session_id: 77978 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:47 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 9380 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #490 | Severity: High | Type: Data Exfiltration (Score: 25.4157)

Log Details:

```
syslog_ts: Jan 28 08:15:49 host: servernameabc process: httpd[12345] ip1: 10.86.54.67 ip2: 0.1.0.1 session_id: 87160 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:49 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 14636 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #492 | Severity: High | Type: Data Exfiltration (Score: 27.2261)

```
Log Details:
syslog_ts: Jan 28 08:15:50 host: servernameabc process: httpd[12345] ip1: 10.222.99.32 ip2: 0.1.0.1
session_id: 15070 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:50 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 15106 response_time: 49 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #500 | Severity: High | Type: Data Exfiltration (Score: 22.0320)

```
Log Details:
syslog_ts: Jan 28 08:15:53 host: servernameabc process: httpd[12345] ip1: 10.39.99.16 ip2: 0.1.0.1
session_id: 66372 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:53 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 4792 response_time: 49 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #502 | Severity: High | Type: Data Exfiltration (Score: 27.8481)

```
Log Details:
syslog_ts: Jan 28 08:15:54 host: servernameabc process: httpd[12345] ip1: 10.36.43.102 ip2: 0.1.0.1
session_id: 70898 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:54 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 18223 response_time: 42 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #505 | Severity: High | Type: Data Exfiltration (Score: 22.0961)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:15:56 host: servernameabc process: httpd[12345] ip1: 10.169.186.252 ip2: 0.1.0.1 session_id: 61965 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:56 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 8197 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #506 | Severity: High | Type: Data Exfiltration (Score: 21.0098)

```
Log Details:
syslog_ts: Jan 28 08:15:57 host: servernameabc process: httpd[12345] ip1: 10.37.251.175 ip2: 0.1.0.1 session_id: 53523 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:57 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 4156 response_time: 39 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #507 | Severity: High | Type: Data Exfiltration (Score: 24.0751)

```
Log Details:
syslog_ts: Jan 28 08:15:58 host: servernameabc process: httpd[12345] ip1: 10.217.5.145 ip2: 0.1.0.1 session_id: 99399 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:58 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 13183 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #513 | Severity: High | Type: Data Exfiltration (Score: 23.3881)

```
Log Details:
syslog_ts: Jan 28 08:16:02 host: servernameabc process: httpd[12345] ip1: 10.212.140.210 ip2: 0.1.0.1 session_id: 45707 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:02 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 10637 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #514 | Severity: High | Type: Data Exfiltration (Score: 18.8787)

Log Details:

```
syslog_ts: Jan 28 08:16:03 host: servernameabc process: httpd[12345] ip1: 10.62.124.220 ip2: 0.1.0.1 session_id: 79456 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:03 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 2872 response_time: 27 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #518 | Severity: High | Type: Data Exfiltration (Score: 22.1272)

Log Details:

```
syslog_ts: Jan 28 08:16:06 host: servernameabc process: httpd[12345] ip1: 10.154.188.93 ip2: 0.1.0.1 session_id: 72809 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:06 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 5412 response_time: 39 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #520 | Severity: High | Type: Data Exfiltration (Score: 13.6410)

Log Details:

```
syslog_ts: Jan 28 08:16:08 host: servernameabc process: httpd[12345] ip1: 10.80.194.75 ip2: 0.1.0.1 session_id: 64382 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:08 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 1158 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #522 | Severity: High | Type: Data Exfiltration (Score: 17.6661)

Log Details:

```
syslog_ts: Jan 28 08:16:09 host: servernameabc process: httpd[12345] ip1: 10.125.250.230 ip2: 0.1.0.1 session_id: 39244 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:09 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 3239 response_time: 7 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #527 | Severity: High | Type: Data Exfiltration (Score: 19.0038)

Log Details:

syslog_ts: Jan 28 08:16:15 host: servernameabc process: httpd[12345] ip1: 10.83.111.35 ip2: 0.1.0.1 session_id: 41047 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:15 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 2340 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #528 | Severity: High | Type: Data Exfiltration (Score: 26.5446)

Log Details:

syslog_ts: Jan 28 08:16:15 host: servernameabc process: httpd[12345] ip1: 10.31.133.167 ip2: 0.1.0.1 session_id: 17488 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:15 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 16304 response_time: 27 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #529 | Severity: High | Type: Data Exfiltration (Score: 27.0128)

Log Details:

syslog_ts: Jan 28 08:16:16 host: servernameabc process: httpd[12345] ip1: 10.234.183.43 ip2: 0.1.0.1 session_id: 56185 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:16 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 19701 response_time: 20 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #536 | Severity: High | Type: Data Exfiltration (Score: 26.6099)

Log Details:

```
syslog_ts: Jan 28 08:16:19 host: servernameabc process: httpd[12345] ip1: 10.220.41.176 ip2: 0.1.0.1 session_id: 71142 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:19 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 16945 response_time: 25 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #539 | Severity: High | Type: Data Exfiltration (Score: 19.4336)

Log Details:

```
syslog_ts: Jan 28 08:16:20 host: servernameabc process: httpd[12345] ip1: 10.188.98.94 ip2: 0.1.0.1 session_id: 85020 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:20 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 3757 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #544 | Severity: High | Type: Data Exfiltration (Score: 26.5189)

Log Details:

```
syslog_ts: Jan 28 08:16:23 host: servernameabc process: httpd[12345] ip1: 10.180.255.179 ip2: 0.1.0.1 session_id: 37972 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:23 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 16022 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #547 | Severity: High | Type: Data Exfiltration (Score: 22.7112)

Log Details:

```
syslog_ts: Jan 28 08:16:26 host: servernameabc process: httpd[12345] ip1: 10.102.163.191 ip2: 0.1.0.1 session_id: 54708 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:26 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 5775 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #554 | Severity: High | Type: Data Exfiltration (Score: 28.1213)

```
Log Details:
syslog_ts: Jan 28 08:16:33 host: servernameabc process: httpd[12345] ip1: 10.128.254.149 ip2: 0.1.0.1
session_id: 36861 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:33 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 19614 response_time: 40 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #555 | Severity: High | Type: Data Exfiltration (Score: 21.6956)

```
Log Details:
syslog_ts: Jan 28 08:16:33 host: servernameabc process: httpd[12345] ip1: 10.115.97.8 ip2: 0.1.0.1
session_id: 82534 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:33 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 4509 response_time: 47 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #556 | Severity: High | Type: Data Exfiltration (Score: 24.8905)

```
Log Details:
syslog_ts: Jan 28 08:16:34 host: servernameabc process: httpd[12345] ip1: 10.112.208.10 ip2: 0.1.0.1
session_id: 60328 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:34 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 9776 response_time: 42 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #560 | Severity: High | Type: Data Exfiltration (Score: 19.6324)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:16:38 host: servernameabc process: httpd[12345] ip1: 10.165.230.108 ip2: 0.1.0.1
session_id: 95983 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:38 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 5197 response_time: 7 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #568 | Severity: High | Type: Data Exfiltration (Score: 23.8564)

```
Log Details:
syslog_ts: Jan 28 08:16:45 host: servernameabc process: httpd[12345] ip1: 10.83.100.96 ip2: 0.1.0.1
session_id: 51190 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:45 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 7635 response_time: 44 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #570 | Severity: High | Type: Data Exfiltration (Score: 26.4816)

```
Log Details:
syslog_ts: Jan 28 08:16:47 host: servernameabc process: httpd[12345] ip1: 10.103.80.30 ip2: 0.1.0.1
session_id: 36681 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:47 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 14861 response_time: 34 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #576 | Severity: High | Type: Data Exfiltration (Score: 22.9631)

```
Log Details:
syslog_ts: Jan 28 08:16:52 host: servernameabc process: httpd[12345] ip1: 10.190.189.40 ip2: 0.1.0.1
session_id: 75918 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:52 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 6063 response_time: 47 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #577 | Severity: High | Type: Data Exfiltration (Score: 13.8612)

Log Details:

```
syslog_ts: Jan 28 08:16:52 host: servernameabc process: httpd[12345] ip1: 10.3.188.133 ip2: 0.1.0.1 session_id: 30897 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:52 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 722 response_time: 27 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #579 | Severity: High | Type: Data Exfiltration (Score: 25.4190)

Log Details:

```
syslog_ts: Jan 28 08:16:54 host: servernameabc process: httpd[12345] ip1: 10.79.208.113 ip2: 0.1.0.1 session_id: 38930 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:54 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 17857 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #597 | Severity: High | Type: Data Exfiltration (Score: 26.8487)

Log Details:

```
syslog_ts: Jan 28 08:17:08 host: servernameabc process: httpd[12345] ip1: 10.85.154.231 ip2: 0.1.0.1 session_id: 82536 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:08 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 19960 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #601 | Severity: High | Type: Data Exfiltration (Score: 24.3250)

Log Details:

```
syslog_ts: Jan 28 08:17:11 host: servernameabc process: httpd[12345] ip1: 10.137.86.208 ip2: 0.1.0.1 session_id: 21616 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:11 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 9381 response_time: 34 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #605 | Severity: High | Type: Data Exfiltration (Score: 25.6457)

Log Details:

syslog_ts: Jan 28 08:17:14 host: servernameabc process: httpd[12345] ip1: 10.147.61.68 ip2: 0.1.0.1 session_id: 11747 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:14 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 11195 response_time: 45 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #607 | Severity: High | Type: Data Exfiltration (Score: 27.4607)

Log Details:

syslog_ts: Jan 28 08:17:16 host: servernameabc process: httpd[12345] ip1: 10.184.10.251 ip2: 0.1.0.1 session_id: 98201 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:16 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 15859 response_time: 49 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #611 | Severity: High | Type: Data Exfiltration (Score: 25.5684)

Log Details:

syslog_ts: Jan 28 08:17:20 host: servernameabc process: httpd[12345] ip1: 10.220.138.133 ip2: 0.1.0.1 session_id: 15138 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:20 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 14221 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #612 | Severity: High | Type: Data Exfiltration (Score: 22.8405)

Log Details:

```
syslog_ts: Jan 28 08:17:20 host: servernameabc process: httpd[12345] ip1: 10.136.92.214 ip2: 0.1.0.1 session_id: 10609 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:20 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 6819 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #613 | Severity: High | Type: Data Exfiltration (Score: 22.4808)

Log Details:

```
syslog_ts: Jan 28 08:17:21 host: servernameabc process: httpd[12345] ip1: 10.21.90.32 ip2: 0.1.0.1 session_id: 43301 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:21 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 5694 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #617 | Severity: High | Type: Data Exfiltration (Score: 13.6465)

Log Details:

```
syslog_ts: Jan 28 08:17:24 host: servernameabc process: httpd[12345] ip1: 10.203.66.218 ip2: 0.1.0.1 session_id: 92388 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:24 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 813 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #619 | Severity: High | Type: Data Exfiltration (Score: 24.7568)

Log Details:

```
syslog_ts: Jan 28 08:17:25 host: servernameabc process: httpd[12345] ip1: 10.73.175.230 ip2: 0.1.0.1 session_id: 13874 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:25 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 11812 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #621 | Severity: High | Type: Data Exfiltration (Score: 23.1794)

```
Log Details:
syslog_ts: Jan 28 08:17:26 host: servernameabc process: httpd[12345] ip1: 10.35.14.204 ip2: 0.1.0.1
session_id: 32929 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:26 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 9397 response_time: 16 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #626 | Severity: High | Type: Data Exfiltration (Score: 22.5955)

```
Log Details:
syslog_ts: Jan 28 08:17:30 host: servernameabc process: httpd[12345] ip1: 10.58.248.56 ip2: 0.1.0.1
session_id: 28545 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:30 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 9367 response_time: 10 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #642 | Severity: High | Type: Data Exfiltration (Score: 20.9929)

```
Log Details:
syslog_ts: Jan 28 08:17:44 host: servernameabc process: httpd[12345] ip1: 10.180.69.47 ip2: 0.1.0.1
session_id: 32099 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:44 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 4094 response_time: 40 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #644 | Severity: High | Type: Data Exfiltration (Score: 25.5221)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:17:46 host: servernameabc process: httpd[12345] ip1: 10.157.166.196 ip2: 0.1.0.1 session_id: 77376 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:46 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 19797 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #647 | Severity: High | Type: Data Exfiltration (Score: 24.1714)

```
Log Details:
syslog_ts: Jan 28 08:17:48 host: servernameabc process: httpd[12345] ip1: 10.128.220.14 ip2: 0.1.0.1 session_id: 84044 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:48 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 15008 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #650 | Severity: High | Type: Data Exfiltration (Score: 25.8306)

```
Log Details:
syslog_ts: Jan 28 08:17:51 host: servernameabc process: httpd[12345] ip1: 10.35.226.199 ip2: 0.1.0.1 session_id: 48885 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:51 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 16490 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #651 | Severity: High | Type: Data Exfiltration (Score: 24.4592)

```
Log Details:
syslog_ts: Jan 28 08:17:52 host: servernameabc process: httpd[12345] ip1: 10.41.193.17 ip2: 0.1.0.1 session_id: 36568 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:52 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 14290 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #653 | Severity: High | Type: Data Exfiltration (Score: 26.4759)

Log Details:

```
syslog_ts: Jan 28 08:17:53 host: servernameabc process: httpd[12345] ip1: 10.73.252.127 ip2: 0.1.0.1 session_id: 32534 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:53 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 17162 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #656 | Severity: High | Type: Data Exfiltration (Score: 16.5291)

Log Details:

```
syslog_ts: Jan 28 08:17:55 host: servernameabc process: httpd[12345] ip1: 10.190.90.66 ip2: 0.1.0.1 session_id: 92016 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:55 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 1201 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #662 | Severity: High | Type: Data Exfiltration (Score: 27.3249)

Log Details:

```
syslog_ts: Jan 28 08:18:00 host: servernameabc process: httpd[12345] ip1: 10.224.98.143 ip2: 0.1.0.1 session_id: 37383 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:00 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 16224 response_time: 43 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #670 | Severity: High | Type: Data Exfiltration (Score: 25.1916)

Log Details:

```
syslog_ts: Jan 28 08:18:05 host: servernameabc process: httpd[12345] ip1: 10.246.124.224 ip2: 0.1.0.1 session_id: 18532 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:05 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 16255 response_time: 10 referer:
```

```
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #672 | Severity: High | Type: Data Exfiltration (Score: 16.3615)

```
Log Details:
syslog_ts: Jan 28 08:18:06  host: servernameabc  process: httpd[12345]  ip1: 10.21.145.138  ip2: 0.1.0.1  session_id: 70921  domain: abc.example.net  apache_ts: 28/Jan/2026:08:18:06 +0530  request: POST /api/v1/auth/login HTTP/1.1  status: 200  bytes: 1248  response_time: 39  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #676 | Severity: High | Type: Data Exfiltration (Score: 27.5302)

```
Log Details:
syslog_ts: Jan 28 08:18:09  host: servernameabc  process: httpd[12345]  ip1: 10.234.240.9  ip2: 0.1.0.1  session_id: 73728  domain: abc.example.net  apache_ts: 28/Jan/2026:08:18:09 +0530  request: POST /api/v1/auth/login HTTP/1.1  status: 200  bytes: 17390  response_time: 40  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #680 | Severity: High | Type: Data Exfiltration (Score: 12.3379)

```
Log Details:
syslog_ts: Jan 28 08:18:13  host: servernameabc  process: httpd[12345]  ip1: 10.122.170.156  ip2: 0.1.0.1  session_id: 36339  domain: abc.example.net  apache_ts: 28/Jan/2026:08:18:13 +0530  request: POST /api/v1/auth/login HTTP/1.1  status: 200  bytes: 414  response_time: 31  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #685 | Severity: High | Type: Data Exfiltration (Score: 26.8613)

Log Details:

```
syslog_ts: Jan 28 08:18:17 host: servernameabc process: httpd[12345] ip1: 10.119.142.154 ip2: 0.1.0.1 session_id: 97721 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:17 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 14737 response_time: 43 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #686 | Severity: High | Type: Data Exfiltration (Score: 25.9755)

Log Details:

```
syslog_ts: Jan 28 08:18:18 host: servernameabc process: httpd[12345] ip1: 10.149.32.197 ip2: 0.1.0.1 session_id: 58834 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:18 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 12460 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #696 | Severity: High | Type: Data Exfiltration (Score: 21.8159)

Log Details:

```
syslog_ts: Jan 28 08:18:26 host: servernameabc process: httpd[12345] ip1: 10.149.40.164 ip2: 0.1.0.1 session_id: 12314 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:26 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 5903 response_time: 26 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #700 | Severity: High | Type: Data Exfiltration (Score: 27.4793)

Log Details:

```
syslog_ts: Jan 28 08:18:28 host: servernameabc process: httpd[12345] ip1: 10.55.183.186 ip2: 0.1.0.1 session_id: 61718 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:28 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 19056 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #703 | Severity: High | Type: Data Exfiltration (Score: 26.2386)

Log Details:

```
syslog_ts: Jan 28 08:18:31 host: servernameabc process: httpd[12345] ip1: 10.60.249.81 ip2: 0.1.0.1 session_id: 33022 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:31 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 16579 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #709 | Severity: High | Type: Data Exfiltration (Score: 22.4802)

Log Details:

```
syslog_ts: Jan 28 08:18:35 host: servernameabc process: httpd[12345] ip1: 10.168.49.113 ip2: 0.1.0.1 session_id: 81537 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:35 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 10487 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #712 | Severity: High | Type: Data Exfiltration (Score: 26.4486)

Log Details:

```
syslog_ts: Jan 28 08:18:38 host: servernameabc process: httpd[12345] ip1: 10.83.188.217 ip2: 0.1.0.1 session_id: 73708 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:38 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 12834 response_time: 49 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #713 | Severity: High | Type: Data Exfiltration (Score: 24.4916)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:18:38 host: servernameabc process: httpd[12345] ip1: 10.79.153.166 ip2: 0.1.0.1 session_id: 72823 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:38 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 12931 response_time: 14 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #714 | Severity: High | Type: Data Exfiltration (Score: 25.8731)

Log Details:

```
syslog_ts: Jan 28 08:18:40 host: servernameabc process: httpd[12345] ip1: 10.95.172.165 ip2: 0.1.0.1 session_id: 81324 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:40 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 18290 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #716 | Severity: High | Type: Data Exfiltration (Score: 24.3753)

Log Details:

```
syslog_ts: Jan 28 08:18:41 host: servernameabc process: httpd[12345] ip1: 10.67.63.52 ip2: 0.1.0.1 session_id: 32336 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:41 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 10587 response_time: 25 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #717 | Severity: High | Type: Data Exfiltration (Score: 19.3067)

Log Details:

```
syslog_ts: Jan 28 08:18:42 host: servernameabc process: httpd[12345] ip1: 10.70.201.23 ip2: 0.1.0.1 session_id: 79776 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:42 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 3400 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #718 | Severity: High | Type: Data Exfiltration (Score: 26.8490)

Log Details:

```
syslog_ts: Jan 28 08:18:43 host: servernameabc process: httpd[12345] ip1: 10.42.170.142 ip2: 0.1.0.1 session_id: 40062 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:43 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 18784 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #728 | Severity: High | Type: Data Exfiltration (Score: 14.2946)

Log Details:

```
syslog_ts: Jan 28 08:18:52 host: servernameabc process: httpd[12345] ip1: 10.182.80.250 ip2: 0.1.0.1 session_id: 72216 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:52 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 984 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #729 | Severity: High | Type: Data Exfiltration (Score: 26.2672)

Log Details:

```
syslog_ts: Jan 28 08:18:53 host: servernameabc process: httpd[12345] ip1: 10.187.21.181 ip2: 0.1.0.1 session_id: 55831 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:53 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 15789 response_time: 25 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #731 | Severity: High | Type: Data Exfiltration (Score: 20.8459)

Log Details:

```
syslog_ts: Jan 28 08:18:55 host: servernameabc process: httpd[12345] ip1: 10.171.187.24 ip2: 0.1.0.1 session_id: 62546 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:55 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 5909 response_time: 13 referer:
```

```
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #735 | Severity: High | Type: Data Exfiltration (Score: 13.8649)

```
Log Details:
syslog_ts: Jan 28 08:18:59  host: servernameabc  process: httpd[12345]  ip1: 10.84.13.230  ip2: 0.1.0.1  session_id: 33013  domain: abc.example.net  apache_ts: 28/Jan/2026:08:18:59 +0530  request: POST /api/v1/auth/login HTTP/1.1  status: 200  bytes: 957  response_time: 14  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #738 | Severity: High | Type: Data Exfiltration (Score: 18.5340)

```
Log Details:
syslog_ts: Jan 28 08:19:01  host: servernameabc  process: httpd[12345]  ip1: 10.213.103.43  ip2: 0.1.0.1  session_id: 71246  domain: abc.example.net  apache_ts: 28/Jan/2026:08:19:01 +0530  request: POST /leaverest/rest/lwpBatch HTTP/1.1  status: 200  bytes: 4004  response_time: 7  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #739 | Severity: High | Type: Data Exfiltration (Score: 21.7484)

```
Log Details:
syslog_ts: Jan 28 08:19:01  host: servernameabc  process: httpd[12345]  ip1: 10.51.199.118  ip2: 0.1.0.1  session_id: 24190  domain: abc.example.net  apache_ts: 28/Jan/2026:08:19:01 +0530  request: POST /api/v1/auth/login HTTP/1.1  status: 200  bytes: 5242  response_time: 34  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #741 | Severity: High | Type: Data Exfiltration (Score: 24.5562)

Log Details:

```
syslog_ts: Jan 28 08:19:02 host: servernameabc process: httpd[12345] ip1: 10.112.95.123 ip2: 0.1.0.1 session_id: 60228 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:02 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 10587 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #743 | Severity: High | Type: Data Exfiltration (Score: 24.7067)

Log Details:

```
syslog_ts: Jan 28 08:19:04 host: servernameabc process: httpd[12345] ip1: 10.50.190.1 ip2: 0.1.0.1 session_id: 34367 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:04 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 10194 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #746 | Severity: High | Type: Data Exfiltration (Score: 23.6010)

Log Details:

```
syslog_ts: Jan 28 08:19:05 host: servernameabc process: httpd[12345] ip1: 10.241.8.57 ip2: 0.1.0.1 session_id: 44907 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:05 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 13319 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #755 | Severity: High | Type: Data Exfiltration (Score: 20.7188)

Log Details:

```
syslog_ts: Jan 28 08:19:13 host: servernameabc process: httpd[12345] ip1: 10.96.84.24 ip2: 0.1.0.1 session_id: 91290 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:13 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 5197 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #757 | Severity: High | Type: Data Exfiltration (Score: 18.3071)

Log Details:

```
syslog_ts: Jan 28 08:19:15 host: servernameabc process: httpd[12345] ip1: 10.19.58.58 ip2: 0.1.0.1 session_id: 48261 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:15 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 2193 response_time: 36 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #759 | Severity: High | Type: Data Exfiltration (Score: 24.3896)

Log Details:

```
syslog_ts: Jan 28 08:19:16 host: servernameabc process: httpd[12345] ip1: 10.132.197.6 ip2: 0.1.0.1 session_id: 74355 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:16 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 11243 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #760 | Severity: High | Type: Data Exfiltration (Score: 17.6824)

Log Details:

```
syslog_ts: Jan 28 08:19:17 host: servernameabc process: httpd[12345] ip1: 10.15.214.128 ip2: 0.1.0.1 session_id: 25138 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:17 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 3483 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #761 | Severity: High | Type: Data Exfiltration (Score: 19.3831)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:19:18 host: servernameabc process: httpd[12345] ip1: 10.150.54.236 ip2: 0.1.0.1
session_id: 93124 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:18 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 4288 response_time: 12 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #764 | Severity: High | Type: Data Exfiltration (Score: 26.7857)

```
Log Details:
syslog_ts: Jan 28 08:19:19 host: servernameabc process: httpd[12345] ip1: 10.161.63.150 ip2: 0.1.0.1
session_id: 65432 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:19 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 18284 response_time: 22 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #768 | Severity: High | Type: Data Exfiltration (Score: 19.5477)

```
Log Details:
syslog_ts: Jan 28 08:19:21 host: servernameabc process: httpd[12345] ip1: 10.104.229.182 ip2: 0.1.0.1
session_id: 10180 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:21 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 4174 response_time: 15 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #773 | Severity: High | Type: Data Exfiltration (Score: 22.7428)

```
Log Details:
syslog_ts: Jan 28 08:19:23 host: servernameabc process: httpd[12345] ip1: 10.7.215.162 ip2: 0.1.0.1
session_id: 12179 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:23 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 7723 response_time: 22 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #774 | Severity: High | Type: Data Exfiltration (Score: 27.2662)

```
Log Details:
syslog_ts: Jan 28 08:19:25 host: servernameabc process: httpd[12345] ip1: 10.160.48.58 ip2: 0.1.0.1
session_id: 95523 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:25 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 19131 response_time: 26 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #780 | Severity: High | Type: Data Exfiltration (Score: 28.2077)

```
Log Details:
syslog_ts: Jan 28 08:19:29 host: servernameabc process: httpd[12345] ip1: 10.135.235.167 ip2: 0.1.0.1
session_id: 23608 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:29 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 19102 response_time: 45 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #784 | Severity: High | Type: Data Exfiltration (Score: 26.4149)

```
Log Details:
syslog_ts: Jan 28 08:19:32 host: servernameabc process: httpd[12345] ip1: 10.53.250.163 ip2: 0.1.0.1
session_id: 17051 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:32 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 14210 response_time: 37 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #789 | Severity: High | Type: Data Exfiltration (Score: 28.0348)

```
Log Details:
syslog_ts: Jan 28 08:19:35 host: servernameabc process: httpd[12345] ip1: 10.133.225.177 ip2: 0.1.0.1
session_id: 29681 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:35 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 18137 response_time: 47 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #792 | Severity: High | Type: Data Exfiltration (Score: 10.0022)

Log Details:

syslog_ts: Jan 28 08:19:38 host: servernameabc process: httpd[12345] ip1: 10.209.45.80 ip2: 0.1.0.1 session_id: 98630 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:38 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 307 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #793 | Severity: High | Type: Data Exfiltration (Score: 25.3106)

Log Details:

syslog_ts: Jan 28 08:19:40 host: servernameabc process: httpd[12345] ip1: 10.161.51.227 ip2: 0.1.0.1 session_id: 24296 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:40 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 14556 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #798 | Severity: High | Type: Data Exfiltration (Score: 25.4844)

Log Details:

syslog_ts: Jan 28 08:19:44 host: servernameabc process: httpd[12345] ip1: 10.252.222.247 ip2: 0.1.0.1 session_id: 55760 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:44 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 11221 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #801 | Severity: High | Type: Data Exfiltration (Score: 26.4731)

Log Details:

```
syslog_ts: Jan 28 08:19:46 host: servernameabc process: httpd[12345] ip1: 10.130.252.25 ip2: 0.1.0.1 session_id: 82360 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:46 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 16917 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #802 | Severity: High | Type: Data Exfiltration (Score: 25.8926)

Log Details:

```
syslog_ts: Jan 28 08:19:48 host: servernameabc process: httpd[12345] ip1: 10.213.55.228 ip2: 0.1.0.1 session_id: 62943 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:48 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 16423 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #803 | Severity: High | Type: Data Exfiltration (Score: 18.5208)

Log Details:

```
syslog_ts: Jan 28 08:19:49 host: servernameabc process: httpd[12345] ip1: 10.118.181.128 ip2: 0.1.0.1 session_id: 85013 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:49 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 3322 response_time: 14 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #804 | Severity: High | Type: Data Exfiltration (Score: 12.5462)

Log Details:

```
syslog_ts: Jan 28 08:19:50 host: servernameabc process: httpd[12345] ip1: 10.4.197.98 ip2: 0.1.0.1 session_id: 85520 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:50 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 541 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #812 | Severity: High | Type: Data Exfiltration (Score: 27.1526)

Log Details:

```
syslog_ts: Jan 28 08:19:55 host: servernameabc process: httpd[12345] ip1: 10.70.199.207 ip2: 0.1.0.1 session_id: 16486 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:55 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 15384 response_time: 45 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #813 | Severity: High | Type: Data Exfiltration (Score: 22.3480)

Log Details:

```
syslog_ts: Jan 28 08:19:55 host: servernameabc process: httpd[12345] ip1: 10.154.163.164 ip2: 0.1.0.1 session_id: 16679 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:55 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 8872 response_time: 10 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #814 | Severity: High | Type: Data Exfiltration (Score: 26.8175)

Log Details:

```
syslog_ts: Jan 28 08:19:56 host: servernameabc process: httpd[12345] ip1: 10.184.199.63 ip2: 0.1.0.1 session_id: 52387 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:56 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 15453 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #824 | Severity: High | Type: Data Exfiltration (Score: 26.8009)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:20:05 host: servernameabc process: httpd[12345] ip1: 10.60.5.126 ip2: 0.1.0.1
session_id: 95017 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:05 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 18873 response_time: 20 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #832 | Severity: High | Type: Data Exfiltration (Score: 22.4844)

```
Log Details:
syslog_ts: Jan 28 08:20:10 host: servernameabc process: httpd[12345] ip1: 10.41.136.140 ip2: 0.1.0.1
session_id: 97176 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:10 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 6288 response_time: 33 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #834 | Severity: High | Type: Data Exfiltration (Score: 24.1616)

```
Log Details:
syslog_ts: Jan 28 08:20:11 host: servernameabc process: httpd[12345] ip1: 10.87.235.252 ip2: 0.1.0.1
session_id: 59403 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:11 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 12057 response_time: 14 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #836 | Severity: High | Type: Data Exfiltration (Score: 26.0427)

```
Log Details:
syslog_ts: Jan 28 08:20:12 host: servernameabc process: httpd[12345] ip1: 10.55.226.117 ip2: 0.1.0.1
session_id: 80689 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:12 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 16159 response_time: 20 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #838 | Severity: High | Type: Data Exfiltration (Score: 19.7460)

```
Log Details:
syslog_ts: Jan 28 08:20:13 host: servernameabc process: httpd[12345] ip1: 10.84.4.161 ip2: 0.1.0.1
session_id: 77868 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:13 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 5693 response_time: 5 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #839 | Severity: High | Type: Data Exfiltration (Score: 27.8108)

```
Log Details:
syslog_ts: Jan 28 08:20:14 host: servernameabc process: httpd[12345] ip1: 10.204.174.143 ip2: 0.1.0.1
session_id: 39705 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:14 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 19523 response_time: 34 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #841 | Severity: High | Type: Data Exfiltration (Score: 24.9000)

```
Log Details:
syslog_ts: Jan 28 08:20:16 host: servernameabc process: httpd[12345] ip1: 10.51.41.56 ip2: 0.1.0.1
session_id: 91095 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:16 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 15303 response_time: 10 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #842 | Severity: High | Type: Data Exfiltration (Score: 26.0463)

```
Log Details:
syslog_ts: Jan 28 08:20:16 host: servernameabc process: httpd[12345] ip1: 10.97.104.99 ip2: 0.1.0.1
session_id: 61948 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:16 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 13866 response_time: 32 referer:
```

```
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #844 | Severity: High | Type: Data Exfiltration (Score: 26.6406)

```
Log Details:
syslog_ts: Jan 28 08:20:18  host: servernameabc  process: httpd[12345]  ip1: 10.215.26.249  ip2: 0.1.0.1  session_id: 32984  domain: abc.example.net  apache_ts: 28/Jan/2026:08:20:18 +0530  request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1  status: 200  bytes: 15694  response_time: 32  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #847 | Severity: High | Type: Data Exfiltration (Score: 27.4994)

```
Log Details:
syslog_ts: Jan 28 08:20:20  host: servernameabc  process: httpd[12345]  ip1: 10.89.42.140  ip2: 0.1.0.1  session_id: 54607  domain: abc.example.net  apache_ts: 28/Jan/2026:08:20:20 +0530  request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1  status: 200  bytes: 17782  response_time: 37  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #856 | Severity: High | Type: Data Exfiltration (Score: 24.9324)

```
Log Details:
syslog_ts: Jan 28 08:20:27  host: servernameabc  process: httpd[12345]  ip1: 10.130.3.165  ip2: 0.1.0.1  session_id: 65016  domain: abc.example.net  apache_ts: 28/Jan/2026:08:20:27 +0530  request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1  status: 200  bytes: 9342  response_time: 48  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #865 | Severity: High | Type: Data Exfiltration (Score: 17.0146)

Log Details:

```
syslog_ts: Jan 28 08:20:34 host: servernameabc process: httpd[12345] ip1: 10.127.106.29 ip2: 0.1.0.1 session_id: 55986 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:34 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 2219 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #869 | Severity: High | Type: Data Exfiltration (Score: 23.7804)

Log Details:

```
syslog_ts: Jan 28 08:20:37 host: servernameabc process: httpd[12345] ip1: 10.101.178.134 ip2: 0.1.0.1 session_id: 98202 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:37 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 7968 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #886 | Severity: High | Type: Data Exfiltration (Score: 25.8710)

Log Details:

```
syslog_ts: Jan 28 08:20:51 host: servernameabc process: httpd[12345] ip1: 10.169.78.21 ip2: 0.1.0.1 session_id: 91700 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:51 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 11962 response_time: 43 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #892 | Severity: High | Type: Data Exfiltration (Score: 22.1633)

Log Details:

```
syslog_ts: Jan 28 08:20:55 host: servernameabc process: httpd[12345] ip1: 10.169.222.23 ip2: 0.1.0.1 session_id: 24242 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:55 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 9213 response_time: 7 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #893 | Severity: High | Type: Data Exfiltration (Score: 26.9626)

```
Log Details:
syslog_ts: Jan 28 08:20:55 host: servernameabc process: httpd[12345] ip1: 10.198.82.40 ip2: 0.1.0.1
session_id: 55690 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:55 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 17985 response_time: 26 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #896 | Severity: High | Type: Data Exfiltration (Score: 24.8357)

```
Log Details:
syslog_ts: Jan 28 08:20:56 host: servernameabc process: httpd[12345] ip1: 10.132.247.33 ip2: 0.1.0.1
session_id: 18564 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:56 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 13405 response_time: 16 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #900 | Severity: High | Type: Data Exfiltration (Score: 21.1701)

```
Log Details:
syslog_ts: Jan 28 08:20:58 host: servernameabc process: httpd[12345] ip1: 10.112.123.16 ip2: 0.1.0.1
session_id: 45955 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:58 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 7185 response_time: 8 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #901 | Severity: High | Type: Data Exfiltration (Score: 27.4138)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:20:58 host: servernameabc process: httpd[12345] ip1: 10.76.6.90 ip2: 0.1.0.1
session_id: 85944 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:58 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 15580 response_time: 50 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #902 | Severity: High | Type: Data Exfiltration (Score: 19.3510)

```
Log Details:
syslog_ts: Jan 28 08:20:59 host: servernameabc process: httpd[12345] ip1: 10.229.108.87 ip2: 0.1.0.1
session_id: 15291 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:59 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 5021 response_time: 6 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #906 | Severity: High | Type: Data Exfiltration (Score: 24.9293)

```
Log Details:
syslog_ts: Jan 28 08:21:03 host: servernameabc process: httpd[12345] ip1: 10.62.150.245 ip2: 0.1.0.1
session_id: 41047 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:03 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 11616 response_time: 27 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #911 | Severity: High | Type: Data Exfiltration (Score: 26.2769)

```
Log Details:
syslog_ts: Jan 28 08:21:06 host: servernameabc process: httpd[12345] ip1: 10.163.57.217 ip2: 0.1.0.1
session_id: 42753 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:06 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 12586 response_time: 47 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #912 | Severity: High | Type: Data Exfiltration (Score: 25.8980)

Log Details:

```
syslog_ts: Jan 28 08:21:07 host: servernameabc process: httpd[12345] ip1: 10.180.64.179 ip2: 0.1.0.1 session_id: 52158 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:07 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 17015 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #920 | Severity: High | Type: Data Exfiltration (Score: 18.3394)

Log Details:

```
syslog_ts: Jan 28 08:21:14 host: servernameabc process: httpd[12345] ip1: 10.193.205.220 ip2: 0.1.0.1 session_id: 74511 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:14 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 2331 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #921 | Severity: High | Type: Data Exfiltration (Score: 25.9233)

Log Details:

```
syslog_ts: Jan 28 08:21:15 host: servernameabc process: httpd[12345] ip1: 10.26.244.120 ip2: 0.1.0.1 session_id: 36080 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:15 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 14156 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #924 | Severity: High | Type: Data Exfiltration (Score: 25.1529)

Log Details:

```
syslog_ts: Jan 28 08:21:17 host: servernameabc process: httpd[12345] ip1: 10.83.171.236 ip2: 0.1.0.1 session_id: 59831 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:17 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 12183 response_time: 27 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #925 | Severity: High | Type: Data Exfiltration (Score: 25.3966)

Log Details:

syslog_ts: Jan 28 08:21:18 host: servernameabc process: httpd[12345] ip1: 10.83.175.248 ip2: 0.1.0.1 session_id: 35161 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:18 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 10335 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #927 | Severity: High | Type: Data Exfiltration (Score: 15.7855)

Log Details:

syslog_ts: Jan 28 08:21:20 host: servernameabc process: httpd[12345] ip1: 10.52.19.24 ip2: 0.1.0.1 session_id: 78255 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:20 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 1565 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #929 | Severity: High | Type: Data Exfiltration (Score: 21.9751)

Log Details:

syslog_ts: Jan 28 08:21:22 host: servernameabc process: httpd[12345] ip1: 10.203.118.119 ip2: 0.1.0.1 session_id: 38929 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:22 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 5168 response_time: 40 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #930 | Severity: High | Type: Data Exfiltration (Score: 19.0394)

Log Details:

```
syslog_ts: Jan 28 08:21:23 host: servernameabc process: httpd[12345] ip1: 10.182.53.102 ip2: 0.1.0.1 session_id: 97767 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:23 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 4263 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #932 | Severity: High | Type: Data Exfiltration (Score: 26.6836)

Log Details:

```
syslog_ts: Jan 28 08:21:25 host: servernameabc process: httpd[12345] ip1: 10.123.84.80 ip2: 0.1.0.1 session_id: 14150 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:25 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 19967 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #933 | Severity: High | Type: Data Exfiltration (Score: 24.0986)

Log Details:

```
syslog_ts: Jan 28 08:21:26 host: servernameabc process: httpd[12345] ip1: 10.24.37.21 ip2: 0.1.0.1 session_id: 32577 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:26 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 8295 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #934 | Severity: High | Type: Data Exfiltration (Score: 26.8318)

Log Details:

```
syslog_ts: Jan 28 08:21:26 host: servernameabc process: httpd[12345] ip1: 10.152.205.164 ip2: 0.1.0.1 session_id: 21581 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:26 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 15347 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #943 | Severity: High | Type: Data Exfiltration (Score: 25.6441)

```
Log Details:
syslog_ts: Jan 28 08:21:33 host: servernameabc process: httpd[12345] ip1: 10.222.218.193 ip2: 0.1.0.1
session_id: 78321 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:33 +0530 request: POST
/RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 13350 response_time: 28 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #945 | Severity: High | Type: Data Exfiltration (Score: 22.6615)

```
Log Details:
syslog_ts: Jan 28 08:21:34 host: servernameabc process: httpd[12345] ip1: 10.232.32.179 ip2: 0.1.0.1
session_id: 95971 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:34 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 9285 response_time: 11 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #948 | Severity: High | Type: Data Exfiltration (Score: 25.0107)

```
Log Details:
syslog_ts: Jan 28 08:21:37 host: servernameabc process: httpd[12345] ip1: 10.159.86.3 ip2: 0.1.0.1
session_id: 67667 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:37 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 12131 response_time: 25 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #952 | Severity: High | Type: Data Exfiltration (Score: 21.1542)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:21:38 host: servernameabc process: httpd[12345] ip1: 10.218.172.8 ip2: 0.1.0.1
session_id: 23939 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:38 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 4210 response_time: 41 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #953 | Severity: High | Type: Data Exfiltration (Score: 15.5889)

```
Log Details:
syslog_ts: Jan 28 08:21:39 host: servernameabc process: httpd[12345] ip1: 10.118.138.19 ip2: 0.1.0.1
session_id: 94935 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:39 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 1285 response_time: 23 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #960 | Severity: High | Type: Data Exfiltration (Score: 10.1047)

```
Log Details:
syslog_ts: Jan 28 08:21:45 host: servernameabc process: httpd[12345] ip1: 10.52.177.185 ip2: 0.1.0.1
session_id: 41070 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:45 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 255 response_time: 18 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #963 | Severity: High | Type: Data Exfiltration (Score: 19.5339)

```
Log Details:
syslog_ts: Jan 28 08:21:48 host: servernameabc process: httpd[12345] ip1: 10.0.202.86 ip2: 0.1.0.1
session_id: 60968 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:48 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 200 bytes: 3113 response_time: 33 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #967 | Severity: High | Type: Data Exfiltration (Score: 26.5072)

Log Details:

```
syslog_ts: Jan 28 08:21:49 host: servernameabc process: httpd[12345] ip1: 10.124.175.36 ip2: 0.1.0.1 session_id: 43353 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:49 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 18046 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #969 | Severity: High | Type: Data Exfiltration (Score: 18.3373)

Log Details:

```
syslog_ts: Jan 28 08:21:51 host: servernameabc process: httpd[12345] ip1: 10.191.114.198 ip2: 0.1.0.1 session_id: 90123 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:51 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 3410 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #973 | Severity: High | Type: Data Exfiltration (Score: 20.9827)

Log Details:

```
syslog_ts: Jan 28 08:21:53 host: servernameabc process: httpd[12345] ip1: 10.140.161.91 ip2: 0.1.0.1 session_id: 14562 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:53 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 4323 response_time: 35 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #983 | Severity: High | Type: Data Exfiltration (Score: 26.8634)

Log Details:

```
syslog_ts: Jan 28 08:22:03 host: servernameabc process: httpd[12345] ip1: 10.250.32.117 ip2: 0.1.0.1 session_id: 95444 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:03 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 17848 response_time: 25 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #987 | Severity: High | Type: Data Exfiltration (Score: 26.5834)

Log Details:

syslog_ts: Jan 28 08:22:07 host: servernameabc process: httpd[12345] ip1: 10.199.117.83 ip2: 0.1.0.1 session_id: 81705 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:07 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 14719 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #990 | Severity: High | Type: Data Exfiltration (Score: 19.1216)

Log Details:

syslog_ts: Jan 28 08:22:09 host: servernameabc process: httpd[12345] ip1: 10.162.84.42 ip2: 0.1.0.1 session_id: 19009 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:09 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 4757 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #991 | Severity: High | Type: Data Exfiltration (Score: 18.7044)

Log Details:

syslog_ts: Jan 28 08:22:11 host: servernameabc process: httpd[12345] ip1: 10.211.9.6 ip2: 0.1.0.1 session_id: 97643 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:11 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 4308 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #994 | Severity: High | Type: Data Exfiltration (Score: 23.5995)

Log Details:

```
syslog_ts: Jan 28 08:22:13 host: servernameabc process: httpd[12345] ip1: 10.116.176.156 ip2: 0.1.0.1 session_id: 86314 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:13 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 8180 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #997 | Severity: High | Type: Data Exfiltration (Score: 20.2812)

Log Details:

```
syslog_ts: Jan 28 08:22:14 host: servernameabc process: httpd[12345] ip1: 10.32.221.71 ip2: 0.1.0.1 session_id: 92262 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:14 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 4114 response_time: 26 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #999 | Severity: High | Type: Data Exfiltration (Score: 27.7899)

Log Details:

```
syslog_ts: Jan 28 08:22:17 host: servernameabc process: httpd[12345] ip1: 10.246.2.171 ip2: 0.1.0.1 session_id: 87686 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:17 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 18008 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with abnormal response times and sizes, indicating potential data exfiltration.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #2 | Severity: High | Type: Data Exfiltration (Score: 25.5398)

Log Details:

```
syslog_ts: Jan 28 08:10:03 host: servernameabc process: httpd[12345] ip1: 10.56.5.70 ip2: 0.1.0.1 session_id: 72902 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:03 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 19754 response_time: 7 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #4 | Severity: High | Type: Data Exfiltration (Score: 22.2787)

```
Log Details:
syslog_ts: Jan 28 08:10:04 host: servernameabc process: httpd[12345] ip1: 10.150.68.229 ip2: 0.1.0.1 session_id: 83820 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:04 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 6761 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #6 | Severity: High | Type: Data Exfiltration (Score: 23.0728)

```
Log Details:
syslog_ts: Jan 28 08:10:05 host: servernameabc process: httpd[12345] ip1: 10.213.133.253 ip2: 0.1.0.1 session_id: 32884 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:05 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 7269 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #7 | Severity: High | Type: Data Exfiltration (Score: 24.0512)

```
Log Details:
syslog_ts: Jan 28 08:10:05 host: servernameabc process: httpd[12345] ip1: 10.137.34.214 ip2: 0.1.0.1 session_id: 35186 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:05 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 13205 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #10 | Severity: High | Type: Data Exfiltration (Score: 24.9662)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:10:07 host: servernameabc process: httpd[12345] ip1: 10.66.106.101 ip2: 0.1.0.1 session_id: 56493 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:07 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 14272 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #11 | Severity: High | Type: Data Exfiltration (Score: 13.2977)

Log Details:

```
syslog_ts: Jan 28 08:10:08 host: servernameabc process: httpd[12345] ip1: 10.246.192.74 ip2: 0.1.0.1 session_id: 23565 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:08 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 547 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #12 | Severity: High | Type: Data Exfiltration (Score: 24.4662)

Log Details:

```
syslog_ts: Jan 28 08:10:08 host: servernameabc process: httpd[12345] ip1: 10.14.225.4 ip2: 0.1.0.1 session_id: 79777 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:08 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 11710 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #15 | Severity: High | Type: Data Exfiltration (Score: 22.1524)

Log Details:

```
syslog_ts: Jan 28 08:10:10 host: servernameabc process: httpd[12345] ip1: 10.47.15.51 ip2: 0.1.0.1 session_id: 27726 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:10 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 7916 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #17 | Severity: High | Type: Data Exfiltration (Score: 19.9750)

Log Details:

```
syslog_ts: Jan 28 08:10:12 host: servernameabc process: httpd[12345] ip1: 10.29.3.82 ip2: 0.1.0.1 session_id: 26656 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:12 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 5006 response_time: 14 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #22 | Severity: High | Type: Data Exfiltration (Score: 26.7892)

Log Details:

```
syslog_ts: Jan 28 08:10:16 host: servernameabc process: httpd[12345] ip1: 10.151.197.138 ip2: 0.1.0.1 session_id: 18493 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:16 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 18740 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #23 | Severity: High | Type: Data Exfiltration (Score: 20.6112)

Log Details:

```
syslog_ts: Jan 28 08:10:17 host: servernameabc process: httpd[12345] ip1: 10.58.26.124 ip2: 0.1.0.1 session_id: 70402 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:17 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 5278 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #25 | Severity: High | Type: Data Exfiltration (Score: 25.1995)

Log Details:

```
syslog_ts: Jan 28 08:10:18 host: servernameabc process: httpd[12345] ip1: 10.3.229.13 ip2: 0.1.0.1 session_id: 80891 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:18 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 16102 response_time: 13
```

referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #29 | Severity: High | Type: Data Exfiltration (Score: 25.5416)

Log Details:

syslog_ts: Jan 28 08:10:22 host: servernameabc process: httpd[12345] ip1: 10.123.83.243 ip2: 0.1.0.1 session_id: 45066 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:22 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 16647 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #30 | Severity: High | Type: Data Exfiltration (Score: 20.4035)

Log Details:

syslog_ts: Jan 28 08:10:22 host: servernameabc process: httpd[12345] ip1: 10.33.190.7 ip2: 0.1.0.1 session_id: 93716 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:22 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 6220 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #32 | Severity: High | Type: Data Exfiltration (Score: 22.8063)

Log Details:

syslog_ts: Jan 28 08:10:23 host: servernameabc process: httpd[12345] ip1: 10.75.69.232 ip2: 0.1.0.1 session_id: 74253 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:23 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 6920 response_time: 36 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #37 | Severity: High | Type: Data Exfiltration (Score: 23.0123)

Log Details:

```
syslog_ts: Jan 28 08:10:27 host: servernameabc process: httpd[12345] ip1: 10.172.14.203 ip2: 0.1.0.1 session_id: 94092 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:27 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 7330 response_time: 35 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #38 | Severity: High | Type: Data Exfiltration (Score: 22.6481)

Log Details:

```
syslog_ts: Jan 28 08:10:27 host: servernameabc process: httpd[12345] ip1: 10.177.76.208 ip2: 0.1.0.1 session_id: 37476 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:27 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 7349 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #40 | Severity: High | Type: Data Exfiltration (Score: 27.5002)

Log Details:

```
syslog_ts: Jan 28 08:10:29 host: servernameabc process: httpd[12345] ip1: 10.131.145.211 ip2: 0.1.0.1 session_id: 30445 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:29 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 18024 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #41 | Severity: High | Type: Data Exfiltration (Score: 22.6928)

Log Details:

```
syslog_ts: Jan 28 08:10:30 host: servernameabc process: httpd[12345] ip1: 10.174.39.149 ip2: 0.1.0.1 session_id: 42254 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:30 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 8331 response_time: 20 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #43 | Severity: High | Type: Data Exfiltration (Score: 24.6299)

```
Log Details:
syslog_ts: Jan 28 08:10:31 host: servernameabc process: httpd[12345] ip1: 10.55.145.253 ip2: 0.1.0.1 session_id: 88867 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:31 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 14596 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #45 | Severity: High | Type: Data Exfiltration (Score: 26.7514)

```
Log Details:
syslog_ts: Jan 28 08:10:33 host: servernameabc process: httpd[12345] ip1: 10.239.44.15 ip2: 0.1.0.1 session_id: 97515 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:33 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 15896 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #47 | Severity: High | Type: Data Exfiltration (Score: 13.7177)

```
Log Details:
syslog_ts: Jan 28 08:10:35 host: servernameabc process: httpd[12345] ip1: 10.51.124.218 ip2: 0.1.0.1 session_id: 76007 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:35 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 1180 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #48 | Severity: High | Type: Data Exfiltration (Score: 26.6539)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:10:35 host: servernameabc process: httpd[12345] ip1: 10.162.140.211 ip2: 0.1.0.1 session_id: 51415 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:35 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 18231 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #49 | Severity: High | Type: Data Exfiltration (Score: 26.3541)

Log Details:

```
syslog_ts: Jan 28 08:10:36 host: servernameabc process: httpd[12345] ip1: 10.11.152.211 ip2: 0.1.0.1 session_id: 11159 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:36 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 13373 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #54 | Severity: High | Type: Data Exfiltration (Score: 15.7395)

Log Details:

```
syslog_ts: Jan 28 08:10:40 host: servernameabc process: httpd[12345] ip1: 10.116.186.189 ip2: 0.1.0.1 session_id: 98430 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:40 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 1733 response_time: 14 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #56 | Severity: High | Type: Data Exfiltration (Score: 17.1059)

Log Details:

```
syslog_ts: Jan 28 08:10:41 host: servernameabc process: httpd[12345] ip1: 10.104.61.52 ip2: 0.1.0.1 session_id: 80155 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:41 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 1478 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #57 | Severity: High | Type: Data Exfiltration (Score: 21.3756)

Log Details:

```
syslog_ts: Jan 28 08:10:42 host: servernameabc process: httpd[12345] ip1: 10.141.240.217 ip2: 0.1.0.1 session_id: 21584 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:42 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 8430 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #60 | Severity: High | Type: Data Exfiltration (Score: 27.6326)

Log Details:

```
syslog_ts: Jan 28 08:10:43 host: servernameabc process: httpd[12345] ip1: 10.29.201.27 ip2: 0.1.0.1 session_id: 46700 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:43 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 17161 response_time: 50 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #61 | Severity: High | Type: Data Exfiltration (Score: 23.6097)

Log Details:

```
syslog_ts: Jan 28 08:10:44 host: servernameabc process: httpd[12345] ip1: 10.91.48.199 ip2: 0.1.0.1 session_id: 66945 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:44 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 9098 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #62 | Severity: High | Type: Data Exfiltration (Score: 25.4864)

Log Details:

```
syslog_ts: Jan 28 08:10:45 host: servernameabc process: httpd[12345] ip1: 10.141.220.59 ip2: 0.1.0.1 session_id: 37496 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:45 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 12073 response_time: 39
```

```
referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #63 | Severity: High | Type: Data Exfiltration (Score: 25.5505)

```
Log Details:
syslog_ts: Jan 28 08:10:45 host: servernameabc process: httpd[12345] ip1: 10.189.157.42 ip2: 0.1.0.1 session_id: 17656 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:45 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 13631 response_time: 29 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #64 | Severity: High | Type: Data Exfiltration (Score: 18.9488)

```
Log Details:
syslog_ts: Jan 28 08:10:46 host: servernameabc process: httpd[12345] ip1: 10.142.250.171 ip2: 0.1.0.1 session_id: 14619 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:46 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 2598 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #65 | Severity: High | Type: Data Exfiltration (Score: 26.1533)

```
Log Details:
syslog_ts: Jan 28 08:10:47 host: servernameabc process: httpd[12345] ip1: 10.40.227.1 ip2: 0.1.0.1 session_id: 63924 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:47 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 16676 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #67 | Severity: High | Type: Data Exfiltration (Score: 24.4489)

Log Details:

```
syslog_ts: Jan 28 08:10:49 host: servernameabc process: httpd[12345] ip1: 10.245.100.8 ip2: 0.1.0.1 session_id: 51620 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:49 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 14054 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #73 | Severity: High | Type: Data Exfiltration (Score: 14.2627)

Log Details:

```
syslog_ts: Jan 28 08:10:54 host: servernameabc process: httpd[12345] ip1: 10.106.58.46 ip2: 0.1.0.1 session_id: 34449 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:54 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 834 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #74 | Severity: High | Type: Data Exfiltration (Score: 17.8776)

Log Details:

```
syslog_ts: Jan 28 08:10:55 host: servernameabc process: httpd[12345] ip1: 10.59.160.200 ip2: 0.1.0.1 session_id: 29004 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:55 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 2337 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #76 | Severity: High | Type: Data Exfiltration (Score: 17.8204)

Log Details:

```
syslog_ts: Jan 28 08:10:57 host: servernameabc process: httpd[12345] ip1: 10.119.49.123 ip2: 0.1.0.1 session_id: 23350 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:57 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 3697 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #78 | Severity: High | Type: Data Exfiltration (Score: 25.3084)

```
Log Details:
syslog_ts: Jan 28 08:10:59 host: servernameabc process: httpd[12345] ip1: 10.16.49.11 ip2: 0.1.0.1
session_id: 93692 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:59 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 18372 response_time: 8 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #79 | Severity: High | Type: Data Exfiltration (Score: 25.4279)

```
Log Details:
syslog_ts: Jan 28 08:11:00 host: servernameabc process: httpd[12345] ip1: 10.145.236.242 ip2: 0.1.0.1
session_id: 42633 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:00 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 19844 response_time: 6 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #82 | Severity: High | Type: Data Exfiltration (Score: 21.3261)

```
Log Details:
syslog_ts: Jan 28 08:11:02 host: servernameabc process: httpd[12345] ip1: 10.34.66.68 ip2: 0.1.0.1
session_id: 53057 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:02 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 8608 response_time: 5 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #83 | Severity: High | Type: Data Exfiltration (Score: 23.8752)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:11:02 host: servernameabc process: httpd[12345] ip1: 10.132.222.144 ip2: 0.1.0.1
session_id: 27845 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:02 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 11964 response_time: 14 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #87 | Severity: High | Type: Data Exfiltration (Score: 27.3940)

```
Log Details:
syslog_ts: Jan 28 08:11:05 host: servernameabc process: httpd[12345] ip1: 10.230.9.230 ip2: 0.1.0.1
session_id: 40842 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:05 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 17026 response_time: 45 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #90 | Severity: High | Type: Data Exfiltration (Score: 19.7502)

```
Log Details:
syslog_ts: Jan 28 08:11:07 host: servernameabc process: httpd[12345] ip1: 10.197.205.235 ip2: 0.1.0.1
session_id: 63028 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:07 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 4469 response_time: 17 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #91 | Severity: High | Type: Data Exfiltration (Score: 24.0029)

```
Log Details:
syslog_ts: Jan 28 08:11:09 host: servernameabc process: httpd[12345] ip1: 10.94.55.191 ip2: 0.1.0.1
session_id: 22977 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:09 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 9133 response_time: 35 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #92 | Severity: High | Type: Data Exfiltration (Score: 22.6875)

```
Log Details:
syslog_ts: Jan 28 08:11:09 host: servernameabc process: httpd[12345] ip1: 10.63.201.2 ip2: 0.1.0.1
session_id: 19303 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:09 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 6262 response_time: 43 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #93 | Severity: High | Type: Data Exfiltration (Score: 25.7095)

```
Log Details:
syslog_ts: Jan 28 08:11:10 host: servernameabc process: httpd[12345] ip1: 10.227.90.195 ip2: 0.1.0.1
session_id: 31405 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:10 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 17231 response_time: 15 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #101 | Severity: High | Type: Data Exfiltration (Score: 18.0599)

```
Log Details:
syslog_ts: Jan 28 08:11:15 host: servernameabc process: httpd[12345] ip1: 10.8.178.53 ip2: 0.1.0.1
session_id: 76562 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:15 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 2696 response_time: 22 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #102 | Severity: High | Type: Data Exfiltration (Score: 20.5490)

```
Log Details:
syslog_ts: Jan 28 08:11:16 host: servernameabc process: httpd[12345] ip1: 10.184.131.147 ip2: 0.1.0.1
session_id: 90378 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:16 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 5497 response_time: 16 referer:
```

Anomaly Detection Report

```
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #106 | Severity: High | Type: Data Exfiltration (Score: 23.3858)

```
Log Details:
syslog_ts: Jan 28 08:11:20  host: servernameabc  process: httpd[12345]  ip1: 10.137.146.152  ip2: 0.1.0.1  session_id:  21257  domain:  abc.example.net  apache_ts:  28/Jan/2026:08:11:20  +0530  request:  GET /dashboard/stats  HTTP/1.1  status:  200  bytes:  13417  response_time:  5  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #110 | Severity: High | Type: Data Exfiltration (Score: 21.2956)

```
Log Details:
syslog_ts: Jan 28 08:11:21  host: servernameabc  process: httpd[12345]  ip1: 10.172.131.162  ip2: 0.1.0.1  session_id:  91188  domain:  abc.example.net  apache_ts:  28/Jan/2026:08:11:21  +0530  request:  GET /timesheet/resources/lib/js/json2.js  HTTP/1.1  status:  200  bytes:  6789  response_time:  14  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #111 | Severity: High | Type: Data Exfiltration (Score: 26.6260)

```
Log Details:
syslog_ts: Jan 28 08:11:21  host: servernameabc  process: httpd[12345]  ip1: 10.55.230.234  ip2: 0.1.0.1  session_id:  21909  domain:  abc.example.net  apache_ts:  28/Jan/2026:08:11:21  +0530  request:  GET /timesheet/resources/lib/js/json2.js  HTTP/1.1  status:  200  bytes:  17042  response_time:  29  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #112 | Severity: High | Type: Data Exfiltration (Score: 26.3942)

Log Details:

syslog_ts: Jan 28 08:11:21 host: servernameabc process: httpd[12345] ip1: 10.180.18.83 ip2: 0.1.0.1 session_id: 97177 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:21 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 15536 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #114 | Severity: High | Type: Data Exfiltration (Score: 24.2289)

Log Details:

syslog_ts: Jan 28 08:11:23 host: servernameabc process: httpd[12345] ip1: 10.116.138.27 ip2: 0.1.0.1 session_id: 25769 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:23 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 13708 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #115 | Severity: High | Type: Data Exfiltration (Score: 22.7574)

Log Details:

syslog_ts: Jan 28 08:11:23 host: servernameabc process: httpd[12345] ip1: 10.100.117.150 ip2: 0.1.0.1 session_id: 43224 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:23 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 7954 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #118 | Severity: High | Type: Data Exfiltration (Score: 25.4938)

Log Details:

syslog_ts: Jan 28 08:11:24 host: servernameabc process: httpd[12345] ip1: 10.145.58.58 ip2: 0.1.0.1 session_id: 61305 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:24 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 13633 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #119 | Severity: High | Type: Data Exfiltration (Score: 25.3442)

```
Log Details:
syslog_ts: Jan 28 08:11:25 host: servernameabc process: httpd[12345] ip1: 10.41.45.127 ip2: 0.1.0.1 session_id: 88519 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:25 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 15190 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #121 | Severity: High | Type: Data Exfiltration (Score: 24.4598)

```
Log Details:
syslog_ts: Jan 28 08:11:26 host: servernameabc process: httpd[12345] ip1: 10.146.204.67 ip2: 0.1.0.1 session_id: 69234 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:26 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 12416 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #123 | Severity: High | Type: Data Exfiltration (Score: 24.3793)

```
Log Details:
syslog_ts: Jan 28 08:11:28 host: servernameabc process: httpd[12345] ip1: 10.74.11.52 ip2: 0.1.0.1 session_id: 38255 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:28 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 11335 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #127 | Severity: High | Type: Data Exfiltration (Score: 26.9126)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:11:30 host: servernameabc process: httpd[12345] ip1: 10.150.241.138 ip2: 0.1.0.1 session_id: 21046 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:30 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 19738 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #128 | Severity: High | Type: Data Exfiltration (Score: 22.1868)

Log Details:

```
syslog_ts: Jan 28 08:11:31 host: servernameabc process: httpd[12345] ip1: 10.23.86.146 ip2: 0.1.0.1 session_id: 18559 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:31 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 10070 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #135 | Severity: High | Type: Data Exfiltration (Score: 20.7992)

Log Details:

```
syslog_ts: Jan 28 08:11:36 host: servernameabc process: httpd[12345] ip1: 10.144.183.99 ip2: 0.1.0.1 session_id: 98602 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:36 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 5164 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #139 | Severity: High | Type: Data Exfiltration (Score: 25.2783)

Log Details:

```
syslog_ts: Jan 28 08:11:38 host: servernameabc process: httpd[12345] ip1: 10.198.19.249 ip2: 0.1.0.1 session_id: 12923 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:38 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 13534 response_time: 25 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #140 | Severity: High | Type: Data Exfiltration (Score: 19.7453)

Log Details:

```
syslog_ts: Jan 28 08:11:38 host: servernameabc process: httpd[12345] ip1: 10.28.135.202 ip2: 0.1.0.1 session_id: 63609 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:38 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 5077 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #142 | Severity: High | Type: Data Exfiltration (Score: 24.0866)

Log Details:

```
syslog_ts: Jan 28 08:11:40 host: servernameabc process: httpd[12345] ip1: 10.134.142.215 ip2: 0.1.0.1 session_id: 94754 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:40 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 13928 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #143 | Severity: High | Type: Data Exfiltration (Score: 28.1763)

Log Details:

```
syslog_ts: Jan 28 08:11:40 host: servernameabc process: httpd[12345] ip1: 10.211.39.72 ip2: 0.1.0.1 session_id: 31816 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:40 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 19325 response_time: 49 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #148 | Severity: High | Type: Data Exfiltration (Score: 23.7458)

Log Details:

```
syslog_ts: Jan 28 08:11:44 host: servernameabc process: httpd[12345] ip1: 10.162.225.200 ip2: 0.1.0.1 session_id: 80727 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:44 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 11019 response_time: 17 referer:
```

```
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #149 | Severity: High | Type: Data Exfiltration (Score: 21.2204)

```
Log Details:
syslog_ts: Jan 28 08:11:45  host: servernameabc  process: httpd[12345]  ip1: 10.37.150.23  ip2: 0.1.0.1  session_id: 58453  domain: abc.example.net  apache_ts: 28/Jan/2026:08:11:45 +0530  request: GET /dashboard/stats HTTP/1.1  status: 200  bytes: 5096  response_time: 31  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #150 | Severity: High | Type: Data Exfiltration (Score: 23.7317)

```
Log Details:
syslog_ts: Jan 28 08:11:47  host: servernameabc  process: httpd[12345]  ip1: 10.107.183.190  ip2: 0.1.0.1  session_id: 26421  domain: abc.example.net  apache_ts: 28/Jan/2026:08:11:47 +0530  request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1  status: 200  bytes: 11834  response_time: 13  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #152 | Severity: High | Type: Data Exfiltration (Score: 25.5422)

```
Log Details:
syslog_ts: Jan 28 08:11:48  host: servernameabc  process: httpd[12345]  ip1: 10.247.252.43  ip2: 0.1.0.1  session_id: 53006  domain: abc.example.net  apache_ts: 28/Jan/2026:08:11:48 +0530  request: GET /dashboard/stats HTTP/1.1  status: 200  bytes: 11872  response_time: 42  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #157 | Severity: High | Type: Data Exfiltration (Score: 26.7954)

Log Details:

```
syslog_ts: Jan 28 08:11:53 host: servernameabc process: httpd[12345] ip1: 10.226.129.56 ip2: 0.1.0.1 session_id: 42570 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:53 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 18523 response_time: 25 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #158 | Severity: High | Type: Data Exfiltration (Score: 27.8638)

Log Details:

```
syslog_ts: Jan 28 08:11:53 host: servernameabc process: httpd[12345] ip1: 10.209.223.159 ip2: 0.1.0.1 session_id: 91067 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:53 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 18741 response_time: 45 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #161 | Severity: High | Type: Data Exfiltration (Score: 24.0061)

Log Details:

```
syslog_ts: Jan 28 08:11:56 host: servernameabc process: httpd[12345] ip1: 10.210.52.231 ip2: 0.1.0.1 session_id: 97252 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:56 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 8193 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #162 | Severity: High | Type: Data Exfiltration (Score: 25.4242)

Log Details:

```
syslog_ts: Jan 28 08:11:57 host: servernameabc process: httpd[12345] ip1: 10.121.170.53 ip2: 0.1.0.1 session_id: 84257 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:57 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 12033 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #163 | Severity: High | Type: Data Exfiltration (Score: 25.8996)

```
Log Details:
syslog_ts: Jan 28 08:11:58  host: servernameabc  process: httpd[12345]  ip1: 10.235.253.140  ip2: 0.1.0.1
session_id: 23682  domain: abc.example.net  apache_ts: 28/Jan/2026:08:11:58 +0530  request: GET /favicon.ico
HTTP/1.1  status: 200  bytes: 13051  response_time: 40  referer: https://abc.example.com/index.html
user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0
Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #165 | Severity: High | Type: Data Exfiltration (Score: 24.7850)

```
Log Details:
syslog_ts: Jan 28 08:12:00  host: servernameabc  process: httpd[12345]  ip1: 10.173.71.123  ip2: 0.1.0.1
session_id:  68479  domain:  abc.example.net  apache_ts:  28/Jan/2026:08:12:00  +0530  request:  GET
/leave/appResources/images/lerf_default.png HTTP/1.1  status: 200  bytes: 11452  response_time: 30  referer:
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #166 | Severity: High | Type: Data Exfiltration (Score: 20.8997)

```
Log Details:
syslog_ts: Jan 28 08:12:00  host: servernameabc  process: httpd[12345]  ip1: 10.159.66.109  ip2: 0.1.0.1
session_id:  65613  domain:  abc.example.net  apache_ts:  28/Jan/2026:08:12:00  +0530  request:  GET
/leave/appResources/images/lerf_default.png HTTP/1.1  status: 200  bytes: 4787  response_time: 30  referer:
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #169 | Severity: High | Type: Data Exfiltration (Score: 19.2465)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:12:04 host: servernameabc process: httpd[12345] ip1: 10.194.30.121 ip2: 0.1.0.1
session_id: 86609 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:04 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 4513 response_time: 11 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #174 | Severity: High | Type: Data Exfiltration (Score: 21.7604)

```
Log Details:
syslog_ts: Jan 28 08:12:08 host: servernameabc process: httpd[12345] ip1: 10.90.166.129 ip2: 0.1.0.1
session_id: 88911 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:08 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 5707 response_time: 32 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #177 | Severity: High | Type: Data Exfiltration (Score: 23.8957)

```
Log Details:
syslog_ts: Jan 28 08:12:10 host: servernameabc process: httpd[12345] ip1: 10.179.183.80 ip2: 0.1.0.1
session_id: 10155 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:10 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 11792 response_time: 15
referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #180 | Severity: High | Type: Data Exfiltration (Score: 25.0293)

```
Log Details:
syslog_ts: Jan 28 08:12:12 host: servernameabc process: httpd[12345] ip1: 10.41.240.117 ip2: 0.1.0.1
session_id: 20608 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:12 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 11288 response_time: 36
referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #181 | Severity: High | Type: Data Exfiltration (Score: 23.8631)

Log Details:

syslog_ts: Jan 28 08:12:12 host: servernameabc process: httpd[12345] ip1: 10.170.131.158 ip2: 0.1.0.1 session_id: 20274 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:12 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 9497 response_time: 29 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #183 | Severity: High | Type: Data Exfiltration (Score: 18.1770)

Log Details:

syslog_ts: Jan 28 08:12:13 host: servernameabc process: httpd[12345] ip1: 10.248.44.155 ip2: 0.1.0.1 session_id: 16846 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:13 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 2105 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #185 | Severity: High | Type: Data Exfiltration (Score: 19.3088)

Log Details:

syslog_ts: Jan 28 08:12:15 host: servernameabc process: httpd[12345] ip1: 10.186.67.154 ip2: 0.1.0.1 session_id: 50570 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:15 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 4823 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #188 | Severity: High | Type: Data Exfiltration (Score: 24.9746)

Log Details:

syslog_ts: Jan 28 08:12:16 host: servernameabc process: httpd[12345] ip1: 10.118.28.11 ip2: 0.1.0.1 session_id: 69371 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:16 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 14297 response_time: 17 referer:

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #189 | Severity: High | Type: Data Exfiltration (Score: 19.4910)

Log Details:

syslog_ts: Jan 28 08:12:17 host: servernameabc process: httpd[12345] ip1: 10.238.43.55 ip2: 0.1.0.1 session_id: 81152 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:17 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 5176 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #190 | Severity: High | Type: Data Exfiltration (Score: 21.1557)

Log Details:

syslog_ts: Jan 28 08:12:19 host: servernameabc process: httpd[12345] ip1: 10.62.239.110 ip2: 0.1.0.1 session_id: 97466 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:19 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 5611 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #193 | Severity: High | Type: Data Exfiltration (Score: 21.8490)

Log Details:

syslog_ts: Jan 28 08:12:21 host: servernameabc process: httpd[12345] ip1: 10.182.51.254 ip2: 0.1.0.1 session_id: 82835 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:21 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 6213 response_time: 27 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #194 | Severity: High | Type: Data Exfiltration (Score: 16.3450)

Log Details:

syslog_ts: Jan 28 08:12:21 host: servernameabc process: httpd[12345] ip1: 10.238.117.37 ip2: 0.1.0.1 session_id: 77765 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:21 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 1283 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #197 | Severity: High | Type: Data Exfiltration (Score: 24.3004)

Log Details:

syslog_ts: Jan 28 08:12:24 host: servernameabc process: httpd[12345] ip1: 10.123.137.114 ip2: 0.1.0.1 session_id: 80625 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:24 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 11302 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #198 | Severity: High | Type: Data Exfiltration (Score: 23.0922)

Log Details:

syslog_ts: Jan 28 08:12:24 host: servernameabc process: httpd[12345] ip1: 10.56.191.129 ip2: 0.1.0.1 session_id: 95484 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:24 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 11571 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #200 | Severity: High | Type: Data Exfiltration (Score: 14.0291)

Log Details:

syslog_ts: Jan 28 08:12:25 host: servernameabc process: httpd[12345] ip1: 10.76.29.203 ip2: 0.1.0.1 session_id: 62232 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:25 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 1334 response_time: 7 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #201 | Severity: High | Type: Data Exfiltration (Score: 26.3032)

Log Details:

```
syslog_ts: Jan 28 08:12:26 host: servernameabc process: httpd[12345] ip1: 10.70.82.63 ip2: 0.1.0.1 session_id: 59359 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:26 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 18216 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #202 | Severity: High | Type: Data Exfiltration (Score: 23.9536)

Log Details:

```
syslog_ts: Jan 28 08:12:27 host: servernameabc process: httpd[12345] ip1: 10.247.63.184 ip2: 0.1.0.1 session_id: 73291 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:27 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 9455 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #209 | Severity: High | Type: Data Exfiltration (Score: 24.8381)

Log Details:

```
syslog_ts: Jan 28 08:12:31 host: servernameabc process: httpd[12345] ip1: 10.178.84.81 ip2: 0.1.0.1 session_id: 28536 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:31 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 15911 response_time: 10 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #210 | Severity: High | Type: Data Exfiltration (Score: 23.9062)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:12:32 host: servernameabc process: httpd[12345] ip1: 10.244.55.60 ip2: 0.1.0.1
session_id: 99385 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:32 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 11606 response_time: 16
referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #212 | Severity: High | Type: Data Exfiltration (Score: 25.4391)

```
Log Details:
syslog_ts: Jan 28 08:12:33 host: servernameabc process: httpd[12345] ip1: 10.252.224.207 ip2: 0.1.0.1
session_id: 69419 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:33 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 13159 response_time: 30
referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #215 | Severity: High | Type: Data Exfiltration (Score: 21.6500)

```
Log Details:
syslog_ts: Jan 28 08:12:36 host: servernameabc process: httpd[12345] ip1: 10.218.76.143 ip2: 0.1.0.1
session_id: 94876 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:36 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 8695 response_time: 7 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #216 | Severity: High | Type: Data Exfiltration (Score: 25.3756)

```
Log Details:
syslog_ts: Jan 28 08:12:37 host: servernameabc process: httpd[12345] ip1: 10.81.88.163 ip2: 0.1.0.1
session_id: 93988 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:37 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 12984 response_time: 30
referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #219 | Severity: High | Type: Data Exfiltration (Score: 26.5771)

```
Log Details:
syslog_ts: Jan 28 08:12:40 host: servernameabc process: httpd[12345] ip1: 10.227.178.248 ip2: 0.1.0.1
session_id: 45171 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:40 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 16872 response_time: 29
referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #221 | Severity: High | Type: Data Exfiltration (Score: 21.7428)

```
Log Details:
syslog_ts: Jan 28 08:12:41 host: servernameabc process: httpd[12345] ip1: 10.51.35.65 ip2: 0.1.0.1
session_id: 53876 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:41 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 7509 response_time: 14 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #222 | Severity: High | Type: Data Exfiltration (Score: 19.5781)

```
Log Details:
syslog_ts: Jan 28 08:12:41 host: servernameabc process: httpd[12345] ip1: 10.182.51.231 ip2: 0.1.0.1
session_id: 88856 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:41 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 4659 response_time: 13 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #224 | Severity: High | Type: Data Exfiltration (Score: 26.2296)

```
Log Details:
syslog_ts: Jan 28 08:12:42 host: servernameabc process: httpd[12345] ip1: 10.145.73.215 ip2: 0.1.0.1
session_id: 23032 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:42 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 19159 response_time: 15 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #226 | Severity: High | Type: Data Exfiltration (Score: 23.4183)

Log Details:

syslog_ts: Jan 28 08:12:43 host: servernameabc process: httpd[12345] ip1: 10.192.40.19 ip2: 0.1.0.1 session_id: 23182 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:43 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 12403 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #228 | Severity: High | Type: Data Exfiltration (Score: 22.3358)

Log Details:

syslog_ts: Jan 28 08:12:44 host: servernameabc process: httpd[12345] ip1: 10.127.29.17 ip2: 0.1.0.1 session_id: 24221 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:44 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 10102 response_time: 7 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #230 | Severity: High | Type: Data Exfiltration (Score: 15.9143)

Log Details:

syslog_ts: Jan 28 08:12:47 host: servernameabc process: httpd[12345] ip1: 10.209.94.42 ip2: 0.1.0.1 session_id: 59799 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:47 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 1282 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #232 | Severity: High | Type: Data Exfiltration (Score: 25.3823)

Log Details:

```
syslog_ts: Jan 28 08:12:48 host: servernameabc process: httpd[12345] ip1: 10.192.111.133 ip2: 0.1.0.1 session_id: 32338 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:48 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 12047 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #233 | Severity: High | Type: Data Exfiltration (Score: 24.4721)

Log Details:

```
syslog_ts: Jan 28 08:12:49 host: servernameabc process: httpd[12345] ip1: 10.25.44.208 ip2: 0.1.0.1 session_id: 35281 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:49 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 11894 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #235 | Severity: High | Type: Data Exfiltration (Score: 22.5175)

Log Details:

```
syslog_ts: Jan 28 08:12:50 host: servernameabc process: httpd[12345] ip1: 10.98.100.72 ip2: 0.1.0.1 session_id: 59609 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:50 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 9295 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #239 | Severity: High | Type: Data Exfiltration (Score: 26.6539)

Log Details:

```
syslog_ts: Jan 28 08:12:53 host: servernameabc process: httpd[12345] ip1: 10.169.251.20 ip2: 0.1.0.1 session_id: 38120 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:53 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 16944 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #241 | Severity: High | Type: Data Exfiltration (Score: 22.9153)

```
Log Details:
syslog_ts: Jan 28 08:12:53 host: servernameabc process: httpd[12345] ip1: 10.111.188.147 ip2: 0.1.0.1 session_id: 16842 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:53 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 6596 response_time: 43 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #243 | Severity: High | Type: Data Exfiltration (Score: 24.2701)

```
Log Details:
syslog_ts: Jan 28 08:12:55 host: servernameabc process: httpd[12345] ip1: 10.183.139.36 ip2: 0.1.0.1 session_id: 62442 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:55 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 10639 response_time: 27 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #244 | Severity: High | Type: Data Exfiltration (Score: 24.8614)

```
Log Details:
syslog_ts: Jan 28 08:12:56 host: servernameabc process: httpd[12345] ip1: 10.168.236.115 ip2: 0.1.0.1 session_id: 76631 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:56 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 13515 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #245 | Severity: High | Type: Data Exfiltration (Score: 17.3126)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:12:56 host: servernameabc process: httpd[12345] ip1: 10.132.238.5 ip2: 0.1.0.1 session_id: 66150 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:56 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 2812 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #247 | Severity: High | Type: Data Exfiltration (Score: 25.4467)

```
Log Details:
syslog_ts: Jan 28 08:12:56 host: servernameabc process: httpd[12345] ip1: 10.30.248.75 ip2: 0.1.0.1 session_id: 84700 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:56 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 11121 response_time: 47 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #249 | Severity: High | Type: Data Exfiltration (Score: 21.3819)

```
Log Details:
syslog_ts: Jan 28 08:12:58 host: servernameabc process: httpd[12345] ip1: 10.57.18.169 ip2: 0.1.0.1 session_id: 32958 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:58 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 4399 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #250 | Severity: High | Type: Data Exfiltration (Score: 21.2715)

```
Log Details:
syslog_ts: Jan 28 08:12:59 host: servernameabc process: httpd[12345] ip1: 10.109.221.70 ip2: 0.1.0.1 session_id: 35833 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:59 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 4747 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #251 | Severity: High | Type: Data Exfiltration (Score: 23.9646)

```
Log Details:
syslog_ts: Jan 28 08:12:59 host: servernameabc process: httpd[12345] ip1: 10.24.14.34 ip2: 0.1.0.1
session_id: 51695 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:59 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 10367 response_time: 24 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #252 | Severity: High | Type: Data Exfiltration (Score: 24.0077)

```
Log Details:
syslog_ts: Jan 28 08:13:00 host: servernameabc process: httpd[12345] ip1: 10.41.175.6 ip2: 0.1.0.1
session_id: 37358 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:00 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 10184 response_time: 26
referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #254 | Severity: High | Type: Data Exfiltration (Score: 21.0795)

```
Log Details:
syslog_ts: Jan 28 08:13:01 host: servernameabc process: httpd[12345] ip1: 10.25.31.36 ip2: 0.1.0.1
session_id: 63622 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:01 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 4994 response_time: 30 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #256 | Severity: High | Type: Data Exfiltration (Score: 27.1724)

```
Log Details:
syslog_ts: Jan 28 08:13:03 host: servernameabc process: httpd[12345] ip1: 10.88.243.43 ip2: 0.1.0.1
session_id: 84691 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:03 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 18231 response_time: 33 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #258 | Severity: High | Type: Data Exfiltration (Score: 19.9889)

Log Details:

syslog_ts: Jan 28 08:13:03 host: servernameabc process: httpd[12345] ip1: 10.217.255.137 ip2: 0.1.0.1 session_id: 92560 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:03 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 3408 response_time: 40 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #263 | Severity: High | Type: Data Exfiltration (Score: 18.9290)

Log Details:

syslog_ts: Jan 28 08:13:06 host: servernameabc process: httpd[12345] ip1: 10.67.83.51 ip2: 0.1.0.1 session_id: 63039 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:06 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 3051 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #265 | Severity: High | Type: Data Exfiltration (Score: 20.0539)

Log Details:

syslog_ts: Jan 28 08:13:07 host: servernameabc process: httpd[12345] ip1: 10.221.7.10 ip2: 0.1.0.1 session_id: 49602 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:07 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 4077 response_time: 27 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #266 | Severity: High | Type: Data Exfiltration (Score: 18.5849)

Log Details:

syslog_ts: Jan 28 08:13:09 host: servernameabc process: httpd[12345] ip1: 10.221.62.224 ip2: 0.1.0.1 session_id: 74993 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:09 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 3076 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #269 | Severity: High | Type: Data Exfiltration (Score: 23.9648)

Log Details:

syslog_ts: Jan 28 08:13:11 host: servernameabc process: httpd[12345] ip1: 10.206.67.89 ip2: 0.1.0.1 session_id: 26455 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:11 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 15144 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #270 | Severity: High | Type: Data Exfiltration (Score: 20.7570)

Log Details:

syslog_ts: Jan 28 08:13:12 host: servernameabc process: httpd[12345] ip1: 10.228.174.202 ip2: 0.1.0.1 session_id: 33817 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:12 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 4690 response_time: 29 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #273 | Severity: High | Type: Data Exfiltration (Score: 21.9274)

Log Details:

syslog_ts: Jan 28 08:13:14 host: servernameabc process: httpd[12345] ip1: 10.247.107.101 ip2: 0.1.0.1 session_id: 35004 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:14 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 5860 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #274 | Severity: High | Type: Data Exfiltration (Score: 24.6294)

```
Log Details:
syslog_ts: Jan 28 08:13:14 host: servernameabc process: httpd[12345] ip1: 10.175.82.44 ip2: 0.1.0.1 session_id: 99522 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:14 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 11349 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #276 | Severity: High | Type: Data Exfiltration (Score: 12.5419)

```
Log Details:
syslog_ts: Jan 28 08:13:15 host: servernameabc process: httpd[12345] ip1: 10.171.42.46 ip2: 0.1.0.1 session_id: 10750 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:15 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 871 response_time: 7 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #280 | Severity: High | Type: Data Exfiltration (Score: 18.1295)

```
Log Details:
syslog_ts: Jan 28 08:13:17 host: servernameabc process: httpd[12345] ip1: 10.219.181.243 ip2: 0.1.0.1 session_id: 24886 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:17 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 2079 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #281 | Severity: High | Type: Data Exfiltration (Score: 25.2985)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:13:18 host: servernameabc process: httpd[12345] ip1: 10.203.63.144 ip2: 0.1.0.1 session_id: 36901 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:18 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 17492 response_time: 10 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #284 | Severity: High | Type: Data Exfiltration (Score: 14.2142)

Log Details:

```
syslog_ts: Jan 28 08:13:20 host: servernameabc process: httpd[12345] ip1: 10.99.44.18 ip2: 0.1.0.1 session_id: 59297 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:20 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 950 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #292 | Severity: High | Type: Data Exfiltration (Score: 23.1945)

Log Details:

```
syslog_ts: Jan 28 08:13:27 host: servernameabc process: httpd[12345] ip1: 10.0.196.183 ip2: 0.1.0.1 session_id: 34464 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:27 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 7811 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #293 | Severity: High | Type: Data Exfiltration (Score: 23.2305)

Log Details:

```
syslog_ts: Jan 28 08:13:28 host: servernameabc process: httpd[12345] ip1: 10.180.218.37 ip2: 0.1.0.1 session_id: 37127 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:28 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 7613 response_time: 36 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #294 | Severity: High | Type: Data Exfiltration (Score: 24.8317)

Log Details:

```
syslog_ts: Jan 28 08:13:28 host: servernameabc process: httpd[12345] ip1: 10.203.99.23 ip2: 0.1.0.1 session_id: 51452 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:28 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 16262 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #296 | Severity: High | Type: Data Exfiltration (Score: 20.6564)

Log Details:

```
syslog_ts: Jan 28 08:13:29 host: servernameabc process: httpd[12345] ip1: 10.244.7.54 ip2: 0.1.0.1 session_id: 67014 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:29 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 5866 response_time: 14 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #297 | Severity: High | Type: Data Exfiltration (Score: 21.3915)

Log Details:

```
syslog_ts: Jan 28 08:13:31 host: servernameabc process: httpd[12345] ip1: 10.101.246.153 ip2: 0.1.0.1 session_id: 88571 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:31 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 5670 response_time: 26 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #298 | Severity: High | Type: Data Exfiltration (Score: 27.8031)

Log Details:

```
syslog_ts: Jan 28 08:13:32 host: servernameabc process: httpd[12345] ip1: 10.226.107.134 ip2: 0.1.0.1 session_id: 46763 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:32 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 17912 response_time: 49
```

referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #299 | Severity: High | Type: Data Exfiltration (Score: 24.3870)

Log Details:

syslog_ts: Jan 28 08:13:32 host: servernameabc process: httpd[12345] ip1: 10.218.19.139 ip2: 0.1.0.1 session_id: 42945 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:32 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 11680 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #300 | Severity: High | Type: Data Exfiltration (Score: 25.7946)

Log Details:

syslog_ts: Jan 28 08:13:33 host: servernameabc process: httpd[12345] ip1: 10.0.129.3 ip2: 0.1.0.1 session_id: 35174 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:33 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 17534 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #302 | Severity: High | Type: Data Exfiltration (Score: 17.6877)

Log Details:

syslog_ts: Jan 28 08:13:34 host: servernameabc process: httpd[12345] ip1: 10.78.50.41 ip2: 0.1.0.1 session_id: 72929 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:34 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 3089 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #305 | Severity: High | Type: Data Exfiltration (Score: 22.5613)

Log Details:

```
syslog_ts: Jan 28 08:13:36 host: servernameabc process: httpd[12345] ip1: 10.197.192.53 ip2: 0.1.0.1 session_id: 18389 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:36 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 9594 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #306 | Severity: High | Type: Data Exfiltration (Score: 26.3955)

Log Details:

```
syslog_ts: Jan 28 08:13:37 host: servernameabc process: httpd[12345] ip1: 10.151.72.189 ip2: 0.1.0.1 session_id: 14251 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:37 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 13840 response_time: 45 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #307 | Severity: High | Type: Data Exfiltration (Score: 17.5152)

Log Details:

```
syslog_ts: Jan 28 08:13:38 host: servernameabc process: httpd[12345] ip1: 10.104.140.191 ip2: 0.1.0.1 session_id: 31445 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:38 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 1878 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #309 | Severity: High | Type: Data Exfiltration (Score: 22.8373)

Log Details:

```
syslog_ts: Jan 28 08:13:39 host: servernameabc process: httpd[12345] ip1: 10.91.223.133 ip2: 0.1.0.1 session_id: 25354 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:39 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 6356 response_time: 45 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #311 | Severity: High | Type: Data Exfiltration (Score: 27.1081)

```
Log Details:
syslog_ts: Jan 28 08:13:40 host: servernameabc process: httpd[12345] ip1: 10.61.168.230 ip2: 0.1.0.1 session_id: 14336 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:40 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 17275 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #314 | Severity: High | Type: Data Exfiltration (Score: 22.2418)

```
Log Details:
syslog_ts: Jan 28 08:13:44 host: servernameabc process: httpd[12345] ip1: 10.58.218.86 ip2: 0.1.0.1 session_id: 71632 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:44 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 6534 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #315 | Severity: High | Type: Data Exfiltration (Score: 24.2472)

```
Log Details:
syslog_ts: Jan 28 08:13:44 host: servernameabc process: httpd[12345] ip1: 10.162.75.133 ip2: 0.1.0.1 session_id: 12154 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:44 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 11867 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #316 | Severity: High | Type: Data Exfiltration (Score: 25.7180)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:13:45 host: servernameabc process: httpd[12345] ip1: 10.88.153.116 ip2: 0.1.0.1 session_id: 91715 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:45 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 16680 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #319 | Severity: High | Type: Data Exfiltration (Score: 17.8321)

Log Details:

```
syslog_ts: Jan 28 08:13:48 host: servernameabc process: httpd[12345] ip1: 10.195.63.254 ip2: 0.1.0.1 session_id: 58224 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:48 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 1992 response_time: 39 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #322 | Severity: High | Type: Data Exfiltration (Score: 24.5455)

Log Details:

```
syslog_ts: Jan 28 08:13:50 host: servernameabc process: httpd[12345] ip1: 10.32.132.61 ip2: 0.1.0.1 session_id: 48053 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:50 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 11745 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #323 | Severity: High | Type: Data Exfiltration (Score: 12.3570)

Log Details:

```
syslog_ts: Jan 28 08:13:51 host: servernameabc process: httpd[12345] ip1: 10.208.167.153 ip2: 0.1.0.1 session_id: 71187 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:51 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 368 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #325 | Severity: High | Type: Data Exfiltration (Score: 12.3869)

Log Details:

```
syslog_ts: Jan 28 08:13:53 host: servernameabc process: httpd[12345] ip1: 10.113.185.117 ip2: 0.1.0.1 session_id: 41947 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:53 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 597 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #329 | Severity: High | Type: Data Exfiltration (Score: 26.7336)

Log Details:

```
syslog_ts: Jan 28 08:13:56 host: servernameabc process: httpd[12345] ip1: 10.7.163.129 ip2: 0.1.0.1 session_id: 64912 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:56 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 16489 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #330 | Severity: High | Type: Data Exfiltration (Score: 23.3070)

Log Details:

```
syslog_ts: Jan 28 08:13:56 host: servernameabc process: httpd[12345] ip1: 10.181.199.69 ip2: 0.1.0.1 session_id: 83600 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:56 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 12801 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #331 | Severity: High | Type: Data Exfiltration (Score: 26.0564)

Log Details:

```
syslog_ts: Jan 28 08:13:57 host: servernameabc process: httpd[12345] ip1: 10.55.232.198 ip2: 0.1.0.1 session_id: 66392 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:57 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 14482 response_time: 33 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #332 | Severity: High | Type: Data Exfiltration (Score: 23.7346)

Log Details:

syslog_ts: Jan 28 08:13:57 host: servernameabc process: httpd[12345] ip1: 10.50.212.249 ip2: 0.1.0.1 session_id: 35258 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:57 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 13261 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #334 | Severity: High | Type: Data Exfiltration (Score: 24.4923)

Log Details:

syslog_ts: Jan 28 08:13:59 host: servernameabc process: httpd[12345] ip1: 10.178.138.224 ip2: 0.1.0.1 session_id: 35053 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:59 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 12705 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #335 | Severity: High | Type: Data Exfiltration (Score: 28.1483)

Log Details:

syslog_ts: Jan 28 08:13:59 host: servernameabc process: httpd[12345] ip1: 10.58.148.156 ip2: 0.1.0.1 session_id: 43508 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:59 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 19065 response_time: 50 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #336 | Severity: High | Type: Data Exfiltration (Score: 20.4472)

Log Details:

```
syslog_ts: Jan 28 08:14:00 host: servernameabc process: httpd[12345] ip1: 10.11.189.19 ip2: 0.1.0.1 session_id: 94862 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:00 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 4544 response_time: 26 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #339 | Severity: High | Type: Data Exfiltration (Score: 27.2812)

Log Details:

```
syslog_ts: Jan 28 08:14:02 host: servernameabc process: httpd[12345] ip1: 10.167.44.68 ip2: 0.1.0.1 session_id: 23761 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:02 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 17725 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #341 | Severity: High | Type: Data Exfiltration (Score: 21.3281)

Log Details:

```
syslog_ts: Jan 28 08:14:03 host: servernameabc process: httpd[12345] ip1: 10.142.90.28 ip2: 0.1.0.1 session_id: 46745 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:03 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 7137 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #342 | Severity: High | Type: Data Exfiltration (Score: 22.2233)

Log Details:

```
syslog_ts: Jan 28 08:14:04 host: servernameabc process: httpd[12345] ip1: 10.113.158.64 ip2: 0.1.0.1 session_id: 12151 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:04 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 5992 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #343 | Severity: High | Type: Data Exfiltration (Score: 26.5883)

```
Log Details:
syslog_ts: Jan 28 08:14:05 host: servernameabc process: httpd[12345] ip1: 10.76.38.130 ip2: 0.1.0.1 session_id: 89193 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:05 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 15368 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #344 | Severity: High | Type: Data Exfiltration (Score: 26.1806)

```
Log Details:
syslog_ts: Jan 28 08:14:05 host: servernameabc process: httpd[12345] ip1: 10.166.168.125 ip2: 0.1.0.1 session_id: 26543 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:05 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 17500 response_time: 20 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #346 | Severity: High | Type: Data Exfiltration (Score: 20.8091)

```
Log Details:
syslog_ts: Jan 28 08:14:08 host: servernameabc process: httpd[12345] ip1: 10.214.61.9 ip2: 0.1.0.1 session_id: 99849 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:08 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 3833 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #350 | Severity: High | Type: Data Exfiltration (Score: 20.1877)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:14:12 host: servernameabc process: httpd[12345] ip1: 10.143.214.218 ip2: 0.1.0.1 session_id: 25628 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:12 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 4335 response_time: 25 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #351 | Severity: High | Type: Data Exfiltration (Score: 21.0035)

```
Log Details:
syslog_ts: Jan 28 08:14:14 host: servernameabc process: httpd[12345] ip1: 10.207.226.61 ip2: 0.1.0.1 session_id: 11043 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:14 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 4666 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #356 | Severity: High | Type: Data Exfiltration (Score: 25.6536)

```
Log Details:
syslog_ts: Jan 28 08:14:18 host: servernameabc process: httpd[12345] ip1: 10.57.187.203 ip2: 0.1.0.1 session_id: 71033 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:18 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 18404 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #358 | Severity: High | Type: Data Exfiltration (Score: 20.4697)

```
Log Details:
syslog_ts: Jan 28 08:14:20 host: servernameabc process: httpd[12345] ip1: 10.45.77.40 ip2: 0.1.0.1 session_id: 66960 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:20 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 5198 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #361 | Severity: High | Type: Data Exfiltration (Score: 11.6457)

```
Log Details:
syslog_ts: Jan 28 08:14:21 host: servernameabc process: httpd[12345] ip1: 10.251.101.45 ip2: 0.1.0.1
session_id: 49270 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:21 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 338 response_time: 34 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #362 | Severity: High | Type: Data Exfiltration (Score: 27.6177)

```
Log Details:
syslog_ts: Jan 28 08:14:22 host: servernameabc process: httpd[12345] ip1: 10.108.190.253 ip2: 0.1.0.1
session_id: 36793 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:22 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 18296 response_time: 42
referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #369 | Severity: High | Type: Data Exfiltration (Score: 19.9113)

```
Log Details:
syslog_ts: Jan 28 08:14:28 host: servernameabc process: httpd[12345] ip1: 10.186.210.186 ip2: 0.1.0.1
session_id: 42143 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:28 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 3236 response_time: 43 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #370 | Severity: High | Type: Data Exfiltration (Score: 25.1663)

```
Log Details:
syslog_ts: Jan 28 08:14:28 host: servernameabc process: httpd[12345] ip1: 10.29.167.169 ip2: 0.1.0.1
session_id: 56204 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:28 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 15405 response_time: 15
```

```
referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #372 | Severity: High | Type: Data Exfiltration (Score: 26.6465)

```
Log Details:
syslog_ts: Jan 28 08:14:29  host: servernameabc  process: httpd[12345]  ip1: 10.224.51.191  ip2: 0.1.0.1  session_id: 94573  domain: abc.example.net  apache_ts: 28/Jan/2026:08:14:29 +0530  request: GET /leave/appResources/images/lerf_default.png HTTP/1.1  status: 200  bytes: 13988  response_time: 50  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #374 | Severity: High | Type: Data Exfiltration (Score: 27.5050)

```
Log Details:
syslog_ts: Jan 28 08:14:31  host: servernameabc  process: httpd[12345]  ip1: 10.151.152.157  ip2: 0.1.0.1  session_id: 12064  domain: abc.example.net  apache_ts: 28/Jan/2026:08:14:31 +0530  request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1  status: 200  bytes: 18553  response_time: 38  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #376 | Severity: High | Type: Data Exfiltration (Score: 25.9376)

```
Log Details:
syslog_ts: Jan 28 08:14:32  host: servernameabc  process: httpd[12345]  ip1: 10.253.200.164  ip2: 0.1.0.1  session_id: 44430  domain: abc.example.net  apache_ts: 28/Jan/2026:08:14:32 +0530  request: GET /leave/appResources/images/lerf_default.png HTTP/1.1  status: 200  bytes: 15531  response_time: 25  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #377 | Severity: High | Type: Data Exfiltration (Score: 23.9472)

Log Details:

```
syslog_ts: Jan 28 08:14:33 host: servernameabc process: httpd[12345] ip1: 10.108.173.23 ip2: 0.1.0.1 session_id: 65098 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:33 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 14643 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #378 | Severity: High | Type: Data Exfiltration (Score: 15.2285)

Log Details:

```
syslog_ts: Jan 28 08:14:33 host: servernameabc process: httpd[12345] ip1: 10.230.72.117 ip2: 0.1.0.1 session_id: 99532 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:33 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 1025 response_time: 35 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #379 | Severity: High | Type: Data Exfiltration (Score: 27.1224)

Log Details:

```
syslog_ts: Jan 28 08:14:33 host: servernameabc process: httpd[12345] ip1: 10.173.129.209 ip2: 0.1.0.1 session_id: 37336 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:33 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 18240 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #380 | Severity: High | Type: Data Exfiltration (Score: 24.6981)

Log Details:

```
syslog_ts: Jan 28 08:14:34 host: servernameabc process: httpd[12345] ip1: 10.57.33.117 ip2: 0.1.0.1 session_id: 20138 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:34 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 11517 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #381 | Severity: High | Type: Data Exfiltration (Score: 21.1499)

```
Log Details:
syslog_ts: Jan 28 08:14:34 host: servernameabc process: httpd[12345] ip1: 10.227.108.57 ip2: 0.1.0.1 session_id: 10435 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:34 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 4084 response_time: 50 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #383 | Severity: High | Type: Data Exfiltration (Score: 20.4548)

```
Log Details:
syslog_ts: Jan 28 08:14:36 host: servernameabc process: httpd[12345] ip1: 10.46.245.131 ip2: 0.1.0.1 session_id: 38624 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:36 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 7087 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #388 | Severity: High | Type: Data Exfiltration (Score: 23.3467)

```
Log Details:
syslog_ts: Jan 28 08:14:40 host: servernameabc process: httpd[12345] ip1: 10.220.165.185 ip2: 0.1.0.1 session_id: 48261 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:40 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 7648 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #390 | Severity: High | Type: Data Exfiltration (Score: 26.3176)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:14:42 host: servernameabc process: httpd[12345] ip1: 10.32.44.242 ip2: 0.1.0.1 session_id: 97114 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:42 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 19171 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #391 | Severity: High | Type: Data Exfiltration (Score: 21.0489)

```
Log Details:
syslog_ts: Jan 28 08:14:42 host: servernameabc process: httpd[12345] ip1: 10.37.7.139 ip2: 0.1.0.1 session_id: 52549 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:42 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 5092 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #393 | Severity: High | Type: Data Exfiltration (Score: 20.3538)

```
Log Details:
syslog_ts: Jan 28 08:14:44 host: servernameabc process: httpd[12345] ip1: 10.163.198.174 ip2: 0.1.0.1 session_id: 30451 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:44 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 3534 response_time: 45 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #394 | Severity: High | Type: Data Exfiltration (Score: 25.9072)

```
Log Details:
syslog_ts: Jan 28 08:14:44 host: servernameabc process: httpd[12345] ip1: 10.131.201.44 ip2: 0.1.0.1 session_id: 11290 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:44 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 14864 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #395 | Severity: High | Type: Data Exfiltration (Score: 23.8854)

Log Details:

```
syslog_ts: Jan 28 08:14:45 host: servernameabc process: httpd[12345] ip1: 10.41.132.29 ip2: 0.1.0.1 session_id: 21057 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:45 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 8363 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #398 | Severity: High | Type: Data Exfiltration (Score: 24.7846)

Log Details:

```
syslog_ts: Jan 28 08:14:47 host: servernameabc process: httpd[12345] ip1: 10.195.11.76 ip2: 0.1.0.1 session_id: 19548 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:47 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 10824 response_time: 35 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #407 | Severity: High | Type: Data Exfiltration (Score: 20.5850)

Log Details:

```
syslog_ts: Jan 28 08:14:53 host: servernameabc process: httpd[12345] ip1: 10.157.105.213 ip2: 0.1.0.1 session_id: 77031 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:53 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 4076 response_time: 37 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #408 | Severity: High | Type: Data Exfiltration (Score: 25.1237)

Log Details:

```
syslog_ts: Jan 28 08:14:54 host: servernameabc process: httpd[12345] ip1: 10.106.156.244 ip2: 0.1.0.1 session_id: 48753 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:54 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 16876 response_time: 10
```

referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #410 | Severity: High | Type: Data Exfiltration (Score: 26.8032)

Log Details:

syslog_ts: Jan 28 08:14:55 host: servernameabc process: httpd[12345] ip1: 10.137.12.246 ip2: 0.1.0.1 session_id: 94149 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:55 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 14815 response_time: 47 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #413 | Severity: High | Type: Data Exfiltration (Score: 26.4581)

Log Details:

syslog_ts: Jan 28 08:14:56 host: servernameabc process: httpd[12345] ip1: 10.195.64.154 ip2: 0.1.0.1 session_id: 21528 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:56 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 14403 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #415 | Severity: High | Type: Data Exfiltration (Score: 27.6194)

Log Details:

syslog_ts: Jan 28 08:14:57 host: servernameabc process: httpd[12345] ip1: 10.91.52.238 ip2: 0.1.0.1 session_id: 14867 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:57 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 18637 response_time: 40 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #416 | Severity: High | Type: Data Exfiltration (Score: 25.5539)

Log Details:

```
syslog_ts: Jan 28 08:14:58 host: servernameabc process: httpd[12345] ip1: 10.35.207.67 ip2: 0.1.0.1 session_id: 58843 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:58 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 11479 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #417 | Severity: High | Type: Data Exfiltration (Score: 22.0942)

Log Details:

```
syslog_ts: Jan 28 08:14:59 host: servernameabc process: httpd[12345] ip1: 10.253.81.149 ip2: 0.1.0.1 session_id: 99166 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:59 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 6239 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #418 | Severity: High | Type: Data Exfiltration (Score: 20.6854)

Log Details:

```
syslog_ts: Jan 28 08:15:00 host: servernameabc process: httpd[12345] ip1: 10.51.56.133 ip2: 0.1.0.1 session_id: 11600 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:00 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 3756 response_time: 47 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #419 | Severity: High | Type: Data Exfiltration (Score: 26.3929)

Log Details:

```
syslog_ts: Jan 28 08:15:00 host: servernameabc process: httpd[12345] ip1: 10.127.63.7 ip2: 0.1.0.1 session_id: 76882 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:00 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 14756 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #420 | Severity: High | Type: Data Exfiltration (Score: 21.6230)

```
Log Details:
syslog_ts: Jan 28 08:15:01 host: servernameabc process: httpd[12345] ip1: 10.80.167.132 ip2: 0.1.0.1 session_id: 41572 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:01 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 5981 response_time: 26 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #423 | Severity: High | Type: Data Exfiltration (Score: 23.9978)

```
Log Details:
syslog_ts: Jan 28 08:15:02 host: servernameabc process: httpd[12345] ip1: 10.19.245.245 ip2: 0.1.0.1 session_id: 80988 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:02 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 10162 response_time: 26 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #426 | Severity: High | Type: Data Exfiltration (Score: 27.1682)

```
Log Details:
syslog_ts: Jan 28 08:15:03 host: servernameabc process: httpd[12345] ip1: 10.162.5.165 ip2: 0.1.0.1 session_id: 27630 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:03 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 16253 response_time: 45 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #427 | Severity: High | Type: Data Exfiltration (Score: 12.3738)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:15:04 host: servernameabc process: httpd[12345] ip1: 10.48.91.12 ip2: 0.1.0.1 session_id: 56075 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:04 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 350 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #428 | Severity: High | Type: Data Exfiltration (Score: 22.0011)

```
Log Details:
syslog_ts: Jan 28 08:15:05 host: servernameabc process: httpd[12345] ip1: 10.109.72.66 ip2: 0.1.0.1 session_id: 48740 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:05 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 8120 response_time: 13 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #430 | Severity: High | Type: Data Exfiltration (Score: 24.0171)

```
Log Details:
syslog_ts: Jan 28 08:15:06 host: servernameabc process: httpd[12345] ip1: 10.108.37.60 ip2: 0.1.0.1 session_id: 69595 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:06 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 10951 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #432 | Severity: High | Type: Data Exfiltration (Score: 23.4618)

```
Log Details:
syslog_ts: Jan 28 08:15:07 host: servernameabc process: httpd[12345] ip1: 10.192.39.157 ip2: 0.1.0.1 session_id: 89424 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:07 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 12518 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #437 | Severity: High | Type: Data Exfiltration (Score: 26.9845)

Log Details:

```
syslog_ts: Jan 28 08:15:11 host: servernameabc process: httpd[12345] ip1: 10.248.143.48 ip2: 0.1.0.1 session_id: 40980 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:11 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 16365 response_time: 40 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #440 | Severity: High | Type: Data Exfiltration (Score: 23.6910)

Log Details:

```
syslog_ts: Jan 28 08:15:13 host: servernameabc process: httpd[12345] ip1: 10.94.250.174 ip2: 0.1.0.1 session_id: 34367 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:13 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 14304 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #441 | Severity: High | Type: Data Exfiltration (Score: 22.0841)

Log Details:

```
syslog_ts: Jan 28 08:15:13 host: servernameabc process: httpd[12345] ip1: 10.184.53.60 ip2: 0.1.0.1 session_id: 18282 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:13 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 5291 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #443 | Severity: High | Type: Data Exfiltration (Score: 21.4400)

Log Details:

```
syslog_ts: Jan 28 08:15:15 host: servernameabc process: httpd[12345] ip1: 10.103.30.210 ip2: 0.1.0.1 session_id: 60808 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:15 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 7162 response_time: 13 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #444 | Severity: High | Type: Data Exfiltration (Score: 21.0582)

Log Details:

syslog_ts: Jan 28 08:15:15 host: servernameabc process: httpd[12345] ip1: 10.15.37.33 ip2: 0.1.0.1 session_id: 70797 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:15 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 4844 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #446 | Severity: High | Type: Data Exfiltration (Score: 17.9191)

Log Details:

syslog_ts: Jan 28 08:15:17 host: servernameabc process: httpd[12345] ip1: 10.211.23.118 ip2: 0.1.0.1 session_id: 19746 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:17 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 3554 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #448 | Severity: High | Type: Data Exfiltration (Score: 17.3814)

Log Details:

syslog_ts: Jan 28 08:15:18 host: servernameabc process: httpd[12345] ip1: 10.27.183.146 ip2: 0.1.0.1 session_id: 86464 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:18 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 1885 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #449 | Severity: High | Type: Data Exfiltration (Score: 17.7642)

Log Details:

```
syslog_ts: Jan 28 08:15:18 host: servernameabc process: httpd[12345] ip1: 10.164.155.12 ip2: 0.1.0.1 session_id: 52716 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:18 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 2236 response_time: 29 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #450 | Severity: High | Type: Data Exfiltration (Score: 22.8195)

Log Details:

```
syslog_ts: Jan 28 08:15:18 host: servernameabc process: httpd[12345] ip1: 10.114.96.136 ip2: 0.1.0.1 session_id: 96542 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:18 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 6156 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #453 | Severity: High | Type: Data Exfiltration (Score: 24.3616)

Log Details:

```
syslog_ts: Jan 28 08:15:20 host: servernameabc process: httpd[12345] ip1: 10.150.167.19 ip2: 0.1.0.1 session_id: 54045 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:20 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 11451 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #455 | Severity: High | Type: Data Exfiltration (Score: 20.5802)

Log Details:

```
syslog_ts: Jan 28 08:15:21 host: servernameabc process: httpd[12345] ip1: 10.34.98.5 ip2: 0.1.0.1 session_id: 63972 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:21 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 7290 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #457 | Severity: High | Type: Data Exfiltration (Score: 27.8031)

Log Details:

```
syslog_ts: Jan 28 08:15:21 host: servernameabc process: httpd[12345] ip1: 10.64.141.177 ip2: 0.1.0.1 session_id: 12125 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:21 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 19345 response_time: 40 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #459 | Severity: High | Type: Data Exfiltration (Score: 15.6166)

Log Details:

```
syslog_ts: Jan 28 08:15:24 host: servernameabc process: httpd[12345] ip1: 10.161.226.35 ip2: 0.1.0.1 session_id: 33799 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:24 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 2048 response_time: 7 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #461 | Severity: High | Type: Data Exfiltration (Score: 25.2452)

Log Details:

```
syslog_ts: Jan 28 08:15:26 host: servernameabc process: httpd[12345] ip1: 10.233.133.26 ip2: 0.1.0.1 session_id: 60112 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:26 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 13621 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #463 | Severity: High | Type: Data Exfiltration (Score: 24.9485)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:15:28 host: servernameabc process: httpd[12345] ip1: 10.137.110.146 ip2: 0.1.0.1 session_id: 77635 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:28 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 14219 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #464 | Severity: High | Type: Data Exfiltration (Score: 26.2182)

Log Details:

```
syslog_ts: Jan 28 08:15:28 host: servernameabc process: httpd[12345] ip1: 10.56.12.26 ip2: 0.1.0.1 session_id: 38916 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:28 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 15487 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #468 | Severity: High | Type: Data Exfiltration (Score: 20.7895)

Log Details:

```
syslog_ts: Jan 28 08:15:29 host: servernameabc process: httpd[12345] ip1: 10.86.31.53 ip2: 0.1.0.1 session_id: 39122 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:29 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 5703 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #469 | Severity: High | Type: Data Exfiltration (Score: 23.3011)

Log Details:

```
syslog_ts: Jan 28 08:15:31 host: servernameabc process: httpd[12345] ip1: 10.200.52.198 ip2: 0.1.0.1 session_id: 71807 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:31 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 7129 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #471 | Severity: High | Type: Data Exfiltration (Score: 25.9174)

Log Details:

```
syslog_ts: Jan 28 08:15:32 host: servernameabc process: httpd[12345] ip1: 10.79.0.159 ip2: 0.1.0.1 session_id: 95248 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:32 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 15466 response_time: 25 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #472 | Severity: High | Type: Data Exfiltration (Score: 26.0278)

Log Details:

```
syslog_ts: Jan 28 08:15:33 host: servernameabc process: httpd[12345] ip1: 10.8.102.5 ip2: 0.1.0.1 session_id: 65168 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:33 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 14554 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #476 | Severity: High | Type: Data Exfiltration (Score: 24.2988)

Log Details:

```
syslog_ts: Jan 28 08:15:36 host: servernameabc process: httpd[12345] ip1: 10.125.204.112 ip2: 0.1.0.1 session_id: 66420 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:36 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 11141 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #481 | Severity: High | Type: Data Exfiltration (Score: 18.0035)

Log Details:

```
syslog_ts: Jan 28 08:15:41 host: servernameabc process: httpd[12345] ip1: 10.232.103.243 ip2: 0.1.0.1 session_id: 21708 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:41 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 2754 response_time: 20 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #484 | Severity: High | Type: Data Exfiltration (Score: 26.3526)

Log Details:

syslog_ts: Jan 28 08:15:44 host: servernameabc process: httpd[12345] ip1: 10.106.184.133 ip2: 0.1.0.1 session_id: 70562 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:44 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 15924 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #494 | Severity: High | Type: Data Exfiltration (Score: 18.7636)

Log Details:

syslog_ts: Jan 28 08:15:51 host: servernameabc process: httpd[12345] ip1: 10.55.238.254 ip2: 0.1.0.1 session_id: 47489 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:51 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 4637 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #495 | Severity: High | Type: Data Exfiltration (Score: 27.0901)

Log Details:

syslog_ts: Jan 28 08:15:51 host: servernameabc process: httpd[12345] ip1: 10.247.213.132 ip2: 0.1.0.1 session_id: 40274 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:51 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 16571 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #497 | Severity: High | Type: Data Exfiltration (Score: 13.8833)

Log Details:

```
syslog_ts: Jan 28 08:15:52 host: servernameabc process: httpd[12345] ip1: 10.53.72.175 ip2: 0.1.0.1 session_id: 12455 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:52 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 1384 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #498 | Severity: High | Type: Data Exfiltration (Score: 26.9458)

Log Details:

```
syslog_ts: Jan 28 08:15:52 host: servernameabc process: httpd[12345] ip1: 10.215.216.164 ip2: 0.1.0.1 session_id: 52790 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:52 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 15797 response_time: 43 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #499 | Severity: High | Type: Data Exfiltration (Score: 21.2504)

Log Details:

```
syslog_ts: Jan 28 08:15:53 host: servernameabc process: httpd[12345] ip1: 10.84.114.164 ip2: 0.1.0.1 session_id: 12740 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:53 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 7958 response_time: 7 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #501 | Severity: High | Type: Data Exfiltration (Score: 18.1700)

Log Details:

```
syslog_ts: Jan 28 08:15:54 host: servernameabc process: httpd[12345] ip1: 10.36.165.186 ip2: 0.1.0.1 session_id: 58539 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:54 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 2348 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #503 | Severity: High | Type: Data Exfiltration (Score: 23.4463)

```
Log Details:
syslog_ts: Jan 28 08:15:55 host: servernameabc process: httpd[12345] ip1: 10.128.149.164 ip2: 0.1.0.1
session_id: 61168 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:55 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 8261 response_time: 33 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #508 | Severity: High | Type: Data Exfiltration (Score: 12.3324)

```
Log Details:
syslog_ts: Jan 28 08:15:58 host: servernameabc process: httpd[12345] ip1: 10.144.244.84 ip2: 0.1.0.1
session_id: 68921 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:58 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 441 response_time: 32 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #509 | Severity: High | Type: Data Exfiltration (Score: 24.1902)

```
Log Details:
syslog_ts: Jan 28 08:15:59 host: servernameabc process: httpd[12345] ip1: 10.243.129.70 ip2: 0.1.0.1
session_id: 27083 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:59 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 13597 response_time: 11 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #512 | Severity: High | Type: Data Exfiltration (Score: 25.5625)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:16:01 host: servernameabc process: httpd[12345] ip1: 10.41.170.212 ip2: 0.1.0.1
session_id: 69550 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:01 +0530 request: GET /favicon.ico
HTTP/1.1 status: 200 bytes: 12915 response_time: 34 referer: https://abc.example.com/index.html
user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko)
Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #515 | Severity: High | Type: Data Exfiltration (Score: 24.5988)

```
Log Details:
syslog_ts: Jan 28 08:16:04 host: servernameabc process: httpd[12345] ip1: 10.226.220.172 ip2: 0.1.0.1
session_id: 50558 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:04 +0530 request: GET /favicon.ico
HTTP/1.1 status: 200 bytes: 12400 response_time: 21 referer: https://abc.example.com/index.html
user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0
Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #516 | Severity: High | Type: Data Exfiltration (Score: 20.7843)

```
Log Details:
syslog_ts: Jan 28 08:16:05 host: servernameabc process: httpd[12345] ip1: 10.215.161.237 ip2: 0.1.0.1
session_id: 28193 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:05 +0530 request: GET /favicon.ico
HTTP/1.1 status: 200 bytes: 5593 response_time: 18 referer: https://abc.example.com/index.html user_agent:
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36
Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #517 | Severity: High | Type: Data Exfiltration (Score: 16.9532)

```
Log Details:
syslog_ts: Jan 28 08:16:06 host: servernameabc process: httpd[12345] ip1: 10.104.100.114 ip2: 0.1.0.1
session_id: 23664 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:06 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 1957 response_time: 24 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #519 | Severity: High | Type: Data Exfiltration (Score: 27.0151)

Log Details:

```
syslog_ts: Jan 28 08:16:08 host: servernameabc process: httpd[12345] ip1: 10.218.165.191 ip2: 0.1.0.1 session_id: 15583 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:08 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 18041 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #521 | Severity: High | Type: Data Exfiltration (Score: 15.5490)

Log Details:

```
syslog_ts: Jan 28 08:16:08 host: servernameabc process: httpd[12345] ip1: 10.168.115.58 ip2: 0.1.0.1 session_id: 66023 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:08 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 1108 response_time: 36 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #523 | Severity: High | Type: Data Exfiltration (Score: 23.6428)

Log Details:

```
syslog_ts: Jan 28 08:16:10 host: servernameabc process: httpd[12345] ip1: 10.225.144.3 ip2: 0.1.0.1 session_id: 30200 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:10 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 11853 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #524 | Severity: High | Type: Data Exfiltration (Score: 23.8228)

Log Details:

```
syslog_ts: Jan 28 08:16:11 host: servernameabc process: httpd[12345] ip1: 10.87.133.227 ip2: 0.1.0.1 session_id: 65784 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:11 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 12066 response_time: 13 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #526 | Severity: High | Type: Data Exfiltration (Score: 25.6133)

Log Details:

syslog_ts: Jan 28 08:16:13 host: servernameabc process: httpd[12345] ip1: 10.227.175.195 ip2: 0.1.0.1 session_id: 68651 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:13 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 16894 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #530 | Severity: High | Type: Data Exfiltration (Score: 21.6163)

Log Details:

syslog_ts: Jan 28 08:16:16 host: servernameabc process: httpd[12345] ip1: 10.198.221.157 ip2: 0.1.0.1 session_id: 37072 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:16 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 4651 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #531 | Severity: High | Type: Data Exfiltration (Score: 19.2659)

Log Details:

syslog_ts: Jan 28 08:16:17 host: servernameabc process: httpd[12345] ip1: 10.130.147.61 ip2: 0.1.0.1 session_id: 46927 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:17 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 3579 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #533 | Severity: High | Type: Data Exfiltration (Score: 27.8777)

Log Details:

```
syslog_ts: Jan 28 08:16:18 host: servernameabc process: httpd[12345] ip1: 10.111.4.220 ip2: 0.1.0.1 session_id: 29389 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:18 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 18955 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #534 | Severity: High | Type: Data Exfiltration (Score: 15.1375)

Log Details:

```
syslog_ts: Jan 28 08:16:18 host: servernameabc process: httpd[12345] ip1: 10.234.189.32 ip2: 0.1.0.1 session_id: 24491 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:18 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 1060 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #535 | Severity: High | Type: Data Exfiltration (Score: 26.7509)

Log Details:

```
syslog_ts: Jan 28 08:16:18 host: servernameabc process: httpd[12345] ip1: 10.59.135.243 ip2: 0.1.0.1 session_id: 92145 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:18 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 14297 response_time: 50 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #537 | Severity: High | Type: Data Exfiltration (Score: 26.6562)

Log Details:

```
syslog_ts: Jan 28 08:16:19 host: servernameabc process: httpd[12345] ip1: 10.234.37.140 ip2: 0.1.0.1 session_id: 97261 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:19 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 14248 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #538 | Severity: High | Type: Data Exfiltration (Score: 21.3936)

Log Details:

```
syslog_ts: Jan 28 08:16:20 host: servernameabc process: httpd[12345] ip1: 10.118.122.217 ip2: 0.1.0.1 session_id: 24552 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:20 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 4370 response_time: 49 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #540 | Severity: High | Type: Data Exfiltration (Score: 18.5662)

Log Details:

```
syslog_ts: Jan 28 08:16:21 host: servernameabc process: httpd[12345] ip1: 10.253.214.20 ip2: 0.1.0.1 session_id: 18324 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:21 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 2707 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #541 | Severity: High | Type: Data Exfiltration (Score: 21.2661)

Log Details:

```
syslog_ts: Jan 28 08:16:22 host: servernameabc process: httpd[12345] ip1: 10.199.43.186 ip2: 0.1.0.1 session_id: 16736 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:22 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 6483 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #542 | Severity: High | Type: Data Exfiltration (Score: 17.6978)

Log Details:

Anomaly Detection Report

syslog_ts: Jan 28 08:16:22 host: servernameabc process: httpd[12345] ip1: 10.12.139.61 ip2: 0.1.0.1 session_id: 94426 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:22 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 1877 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #543 | Severity: High | Type: Data Exfiltration (Score: 22.2263)

Log Details:

syslog_ts: Jan 28 08:16:23 host: servernameabc process: httpd[12345] ip1: 10.34.74.190 ip2: 0.1.0.1 session_id: 75422 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:23 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 6352 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #546 | Severity: High | Type: Data Exfiltration (Score: 21.2588)

Log Details:

syslog_ts: Jan 28 08:16:25 host: servernameabc process: httpd[12345] ip1: 10.184.87.222 ip2: 0.1.0.1 session_id: 70804 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:25 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 6131 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #549 | Severity: High | Type: Data Exfiltration (Score: 24.2729)

Log Details:

syslog_ts: Jan 28 08:16:28 host: servernameabc process: httpd[12345] ip1: 10.240.88.129 ip2: 0.1.0.1 session_id: 25002 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:28 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 12548 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #551 | Severity: High | Type: Data Exfiltration (Score: 19.0477)

```
Log Details:
syslog_ts: Jan 28 08:16:30 host: servernameabc process: httpd[12345] ip1: 10.125.60.212 ip2: 0.1.0.1
session_id: 53887 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:30 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 5129 response_time: 5 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #552 | Severity: High | Type: Data Exfiltration (Score: 27.3626)

```
Log Details:
syslog_ts: Jan 28 08:16:31 host: servernameabc process: httpd[12345] ip1: 10.176.179.128 ip2: 0.1.0.1
session_id: 66825 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:31 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 18563 response_time: 35 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #553 | Severity: High | Type: Data Exfiltration (Score: 26.3953)

```
Log Details:
syslog_ts: Jan 28 08:16:32 host: servernameabc process: httpd[12345] ip1: 10.182.209.105 ip2: 0.1.0.1
session_id: 48023 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:32 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 14910 response_time: 37
referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #558 | Severity: High | Type: Data Exfiltration (Score: 26.5366)

```
Log Details:
syslog_ts: Jan 28 08:16:36 host: servernameabc process: httpd[12345] ip1: 10.129.204.116 ip2: 0.1.0.1
session_id: 82504 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:36 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 14255 response_time: 45
```

referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #561 | Severity: High | Type: Data Exfiltration (Score: 27.6463)

Log Details:

syslog_ts: Jan 28 08:16:39 host: servernameabc process: httpd[12345] ip1: 10.189.109.238 ip2: 0.1.0.1 session_id: 70977 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:39 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 17631 response_time: 47 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #562 | Severity: High | Type: Data Exfiltration (Score: 24.3254)

Log Details:

syslog_ts: Jan 28 08:16:40 host: servernameabc process: httpd[12345] ip1: 10.101.125.13 ip2: 0.1.0.1 session_id: 64826 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:40 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 11699 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #563 | Severity: High | Type: Data Exfiltration (Score: 20.4796)

Log Details:

syslog_ts: Jan 28 08:16:41 host: servernameabc process: httpd[12345] ip1: 10.183.14.65 ip2: 0.1.0.1 session_id: 50998 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:41 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 5118 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #564 | Severity: High | Type: Data Exfiltration (Score: 27.3072)

Log Details:

```
syslog_ts: Jan 28 08:16:41 host: servernameabc process: httpd[12345] ip1: 10.0.13.98 ip2: 0.1.0.1 session_id: 22314 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:41 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 16049 response_time: 50 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #566 | Severity: High | Type: Data Exfiltration (Score: 27.0972)

Log Details:

```
syslog_ts: Jan 28 08:16:43 host: servernameabc process: httpd[12345] ip1: 10.14.140.108 ip2: 0.1.0.1 session_id: 62624 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:43 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 18984 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #567 | Severity: High | Type: Data Exfiltration (Score: 26.2254)

Log Details:

```
syslog_ts: Jan 28 08:16:44 host: servernameabc process: httpd[12345] ip1: 10.110.102.117 ip2: 0.1.0.1 session_id: 21399 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:44 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 14111 response_time: 39 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #569 | Severity: High | Type: Data Exfiltration (Score: 21.8736)

Log Details:

```
syslog_ts: Jan 28 08:16:46 host: servernameabc process: httpd[12345] ip1: 10.43.236.160 ip2: 0.1.0.1 session_id: 97810 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:46 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 6824 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #571 | Severity: High | Type: Data Exfiltration (Score: 25.8492)

```
Log Details:
syslog_ts: Jan 28 08:16:47 host: servernameabc process: httpd[12345] ip1: 10.25.56.30 ip2: 0.1.0.1
session_id: 14778 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:47 +0530 request: GET /favicon.ico
HTTP/1.1 status: 200 bytes: 12120 response_time: 47 referer: https://abc.example.com/index.html
user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko)
Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #574 | Severity: High | Type: Data Exfiltration (Score: 18.4149)

```
Log Details:
syslog_ts: Jan 28 08:16:49 host: servernameabc process: httpd[12345] ip1: 10.35.25.59 ip2: 0.1.0.1
session_id: 71566 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:49 +0530 request: GET /favicon.ico
HTTP/1.1 status: 200 bytes: 2605 response_time: 30 referer: https://abc.example.com/index.html user_agent:
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36
Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #575 | Severity: High | Type: Data Exfiltration (Score: 20.3883)

```
Log Details:
syslog_ts: Jan 28 08:16:50 host: servernameabc process: httpd[12345] ip1: 10.62.86.59 ip2: 0.1.0.1
session_id: 53531 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:50 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 5401 response_time: 15 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #581 | Severity: High | Type: Data Exfiltration (Score: 25.9489)

```
Log Details:
```

Anomaly Detection Report

syslog_ts: Jan 28 08:16:55 host: servernameabc process: httpd[12345] ip1: 10.157.238.76 ip2: 0.1.0.1 session_id: 24019 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:55 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 12942 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #582 | Severity: High | Type: Data Exfiltration (Score: 26.5142)

Log Details:

syslog_ts: Jan 28 08:16:56 host: servernameabc process: httpd[12345] ip1: 10.133.46.97 ip2: 0.1.0.1 session_id: 93034 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:56 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 18204 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #583 | Severity: High | Type: Data Exfiltration (Score: 21.3383)

Log Details:

syslog_ts: Jan 28 08:16:56 host: servernameabc process: httpd[12345] ip1: 10.150.42.220 ip2: 0.1.0.1 session_id: 57599 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:56 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 4438 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #584 | Severity: High | Type: Data Exfiltration (Score: 16.6500)

Log Details:

syslog_ts: Jan 28 08:16:57 host: servernameabc process: httpd[12345] ip1: 10.97.236.4 ip2: 0.1.0.1 session_id: 82062 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:57 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 2204 response_time: 14 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #585 | Severity: High | Type: Data Exfiltration (Score: 14.6518)

```
Log Details:
syslog_ts: Jan 28 08:16:58 host: servernameabc process: httpd[12345] ip1: 10.173.204.201 ip2: 0.1.0.1
session_id: 34708 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:58 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 1001 response_time: 26 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #586 | Severity: High | Type: Data Exfiltration (Score: 27.8696)

```
Log Details:
syslog_ts: Jan 28 08:16:59 host: servernameabc process: httpd[12345] ip1: 10.240.74.248 ip2: 0.1.0.1
session_id: 10361 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:59 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 18157 response_time: 49 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #587 | Severity: High | Type: Data Exfiltration (Score: 18.5295)

```
Log Details:
syslog_ts: Jan 28 08:16:59 host: servernameabc process: httpd[12345] ip1: 10.115.69.7 ip2: 0.1.0.1
session_id: 20643 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:59 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 2844 response_time: 26 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #588 | Severity: High | Type: Data Exfiltration (Score: 21.5749)

```
Log Details:
syslog_ts: Jan 28 08:17:00 host: servernameabc process: httpd[12345] ip1: 10.148.240.149 ip2: 0.1.0.1
session_id: 68139 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:00 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 6180 response_time: 23 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #589 | Severity: High | Type: Data Exfiltration (Score: 24.2365)

Log Details:

syslog_ts: Jan 28 08:17:02 host: servernameabc process: httpd[12345] ip1: 10.183.13.194 ip2: 0.1.0.1 session_id: 19520 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:02 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 8949 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #590 | Severity: High | Type: Data Exfiltration (Score: 14.8735)

Log Details:

syslog_ts: Jan 28 08:17:02 host: servernameabc process: httpd[12345] ip1: 10.131.79.38 ip2: 0.1.0.1 session_id: 88327 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:02 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 862 response_time: 40 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #591 | Severity: High | Type: Data Exfiltration (Score: 16.1087)

Log Details:

syslog_ts: Jan 28 08:17:03 host: servernameabc process: httpd[12345] ip1: 10.59.173.13 ip2: 0.1.0.1 session_id: 45977 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:03 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 1247 response_time: 39 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #592 | Severity: High | Type: Data Exfiltration (Score: 26.8893)

Log Details:

```
syslog_ts: Jan 28 08:17:04 host: servernameabc process: httpd[12345] ip1: 10.115.6.54 ip2: 0.1.0.1 session_id: 17780 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:04 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 19922 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #593 | Severity: High | Type: Data Exfiltration (Score: 26.5787)

Log Details:

```
syslog_ts: Jan 28 08:17:05 host: servernameabc process: httpd[12345] ip1: 10.206.75.223 ip2: 0.1.0.1 session_id: 26957 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:05 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 14381 response_time: 45 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #595 | Severity: High | Type: Data Exfiltration (Score: 14.5852)

Log Details:

```
syslog_ts: Jan 28 08:17:06 host: servernameabc process: httpd[12345] ip1: 10.17.201.234 ip2: 0.1.0.1 session_id: 25797 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:06 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 875 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #596 | Severity: High | Type: Data Exfiltration (Score: 24.6824)

Log Details:

```
syslog_ts: Jan 28 08:17:07 host: servernameabc process: httpd[12345] ip1: 10.88.5.8 ip2: 0.1.0.1 session_id: 41374 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:07 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 11072 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #598 | Severity: High | Type: Data Exfiltration (Score: 24.1234)

Log Details:

```
syslog_ts: Jan 28 08:17:08 host: servernameabc process: httpd[12345] ip1: 10.229.96.133 ip2: 0.1.0.1 session_id: 82316 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:08 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 11204 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #599 | Severity: High | Type: Data Exfiltration (Score: 24.9819)

Log Details:

```
syslog_ts: Jan 28 08:17:10 host: servernameabc process: httpd[12345] ip1: 10.155.125.50 ip2: 0.1.0.1 session_id: 84649 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:10 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 15393 response_time: 13 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #600 | Severity: High | Type: Data Exfiltration (Score: 24.5583)

Log Details:

```
syslog_ts: Jan 28 08:17:11 host: servernameabc process: httpd[12345] ip1: 10.32.139.153 ip2: 0.1.0.1 session_id: 68968 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:11 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 13328 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #602 | Severity: High | Type: Data Exfiltration (Score: 27.8579)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:17:12 host: servernameabc process: httpd[12345] ip1: 10.181.78.70 ip2: 0.1.0.1 session_id: 69090 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:12 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 18879 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #604 | Severity: High | Type: Data Exfiltration (Score: 20.8334)

```
Log Details:
syslog_ts: Jan 28 08:17:14 host: servernameabc process: httpd[12345] ip1: 10.244.104.114 ip2: 0.1.0.1 session_id: 11757 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:14 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 3819 response_time: 49 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #606 | Severity: High | Type: Data Exfiltration (Score: 22.5435)

```
Log Details:
syslog_ts: Jan 28 08:17:15 host: servernameabc process: httpd[12345] ip1: 10.190.91.16 ip2: 0.1.0.1 session_id: 77086 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:15 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 6311 response_time: 39 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #610 | Severity: High | Type: Data Exfiltration (Score: 22.4874)

```
Log Details:
syslog_ts: Jan 28 08:17:19 host: servernameabc process: httpd[12345] ip1: 10.223.126.111 ip2: 0.1.0.1 session_id: 71599 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:19 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 8527 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #614 | Severity: High | Type: Data Exfiltration (Score: 27.9970)

Log Details:

```
syslog_ts: Jan 28 08:17:21 host: servernameabc process: httpd[12345] ip1: 10.31.39.19 ip2: 0.1.0.1 session_id: 59516 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:21 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 18784 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #615 | Severity: High | Type: Data Exfiltration (Score: 13.7777)

Log Details:

```
syslog_ts: Jan 28 08:17:22 host: servernameabc process: httpd[12345] ip1: 10.98.95.61 ip2: 0.1.0.1 session_id: 71170 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:22 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 746 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #616 | Severity: High | Type: Data Exfiltration (Score: 26.6447)

Log Details:

```
syslog_ts: Jan 28 08:17:23 host: servernameabc process: httpd[12345] ip1: 10.169.134.213 ip2: 0.1.0.1 session_id: 16721 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:23 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 14840 response_time: 43 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #620 | Severity: High | Type: Data Exfiltration (Score: 19.4165)

Log Details:

```
syslog_ts: Jan 28 08:17:25 host: servernameabc process: httpd[12345] ip1: 10.136.145.171 ip2: 0.1.0.1 session_id: 18302 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:25 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 3838 response_time: 21 referer:
```

```
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #622 | Severity: High | Type: Data Exfiltration (Score: 26.0175)

```
Log Details:
syslog_ts: Jan 28 08:17:27  host: servernameabc  process: httpd[12345]  ip1: 10.102.25.61  ip2: 0.1.0.1  session_id: 88216  domain: abc.example.net  apache_ts: 28/Jan/2026:08:17:27 +0530  request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1  status: 200  bytes: 16442  response_time: 22  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #623 | Severity: High | Type: Data Exfiltration (Score: 26.4997)

```
Log Details:
syslog_ts: Jan 28 08:17:27  host: servernameabc  process: httpd[12345]  ip1: 10.13.153.248  ip2: 0.1.0.1  session_id: 43365  domain: abc.example.net  apache_ts: 28/Jan/2026:08:17:27 +0530  request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1  status: 200  bytes: 18959  response_time: 19  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #624 | Severity: High | Type: Data Exfiltration (Score: 24.9072)

```
Log Details:
syslog_ts: Jan 28 08:17:28  host: servernameabc  process: httpd[12345]  ip1: 10.150.168.22  ip2: 0.1.0.1  session_id: 32260  domain: abc.example.net  apache_ts: 28/Jan/2026:08:17:28 +0530  request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1  status: 200  bytes: 13436  response_time: 20  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #625 | Severity: High | Type: Data Exfiltration (Score: 20.9521)

Log Details:

syslog_ts: Jan 28 08:17:30 host: servernameabc process: httpd[12345] ip1: 10.175.134.129 ip2: 0.1.0.1 session_id: 38720 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:30 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 5436 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #629 | Severity: High | Type: Data Exfiltration (Score: 23.8244)

Log Details:

syslog_ts: Jan 28 08:17:33 host: servernameabc process: httpd[12345] ip1: 10.234.134.72 ip2: 0.1.0.1 session_id: 62355 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:33 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 12070 response_time: 13 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #630 | Severity: High | Type: Data Exfiltration (Score: 24.0552)

Log Details:

syslog_ts: Jan 28 08:17:34 host: servernameabc process: httpd[12345] ip1: 10.54.185.96 ip2: 0.1.0.1 session_id: 41864 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:34 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 9783 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #631 | Severity: High | Type: Data Exfiltration (Score: 27.3124)

Log Details:

syslog_ts: Jan 28 08:17:35 host: servernameabc process: httpd[12345] ip1: 10.235.84.170 ip2: 0.1.0.1 session_id: 62460 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:35 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 16743 response_time: 45 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #632 | Severity: High | Type: Data Exfiltration (Score: 17.8009)

```
Log Details:
syslog_ts: Jan 28 08:17:36 host: servernameabc process: httpd[12345] ip1: 10.133.42.42 ip2: 0.1.0.1 session_id: 38332 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:36 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 2440 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #633 | Severity: High | Type: Data Exfiltration (Score: 25.2837)

```
Log Details:
syslog_ts: Jan 28 08:17:37 host: servernameabc process: httpd[12345] ip1: 10.163.237.5 ip2: 0.1.0.1 session_id: 48728 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:37 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 14764 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #635 | Severity: High | Type: Data Exfiltration (Score: 21.5624)

```
Log Details:
syslog_ts: Jan 28 08:17:39 host: servernameabc process: httpd[12345] ip1: 10.148.81.130 ip2: 0.1.0.1 session_id: 47855 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:39 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 8785 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #637 | Severity: High | Type: Data Exfiltration (Score: 23.1301)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:17:40 host: servernameabc process: httpd[12345] ip1: 10.126.66.45 ip2: 0.1.0.1 session_id: 62072 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:40 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 8895 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #639 | Severity: High | Type: Data Exfiltration (Score: 25.9941)

```
Log Details:
syslog_ts: Jan 28 08:17:41 host: servernameabc process: httpd[12345] ip1: 10.247.87.123 ip2: 0.1.0.1 session_id: 37720 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:41 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 13994 response_time: 35 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #640 | Severity: High | Type: Data Exfiltration (Score: 24.7715)

```
Log Details:
syslog_ts: Jan 28 08:17:42 host: servernameabc process: httpd[12345] ip1: 10.227.241.35 ip2: 0.1.0.1 session_id: 79508 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:42 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 11419 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #643 | Severity: High | Type: Data Exfiltration (Score: 25.1386)

```
Log Details:
syslog_ts: Jan 28 08:17:44 host: servernameabc process: httpd[12345] ip1: 10.51.82.193 ip2: 0.1.0.1 session_id: 54980 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:44 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 13319 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #648 | Severity: High | Type: Data Exfiltration (Score: 23.4425)

Log Details:

```
syslog_ts: Jan 28 08:17:49 host: servernameabc process: httpd[12345] ip1: 10.94.18.35 ip2: 0.1.0.1 session_id: 92875 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:49 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 12467 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #649 | Severity: High | Type: Data Exfiltration (Score: 24.5502)

Log Details:

```
syslog_ts: Jan 28 08:17:50 host: servernameabc process: httpd[12345] ip1: 10.4.158.14 ip2: 0.1.0.1 session_id: 42433 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:50 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 12460 response_time: 20 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #652 | Severity: High | Type: Data Exfiltration (Score: 23.5268)

Log Details:

```
syslog_ts: Jan 28 08:17:52 host: servernameabc process: httpd[12345] ip1: 10.131.20.32 ip2: 0.1.0.1 session_id: 74284 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:52 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 7646 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #654 | Severity: High | Type: Data Exfiltration (Score: 21.6187)

Log Details:

```
syslog_ts: Jan 28 08:17:53 host: servernameabc process: httpd[12345] ip1: 10.56.81.30 ip2: 0.1.0.1 session_id: 40011 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:53 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 7979 response_time: 10 referer: https://abc.example.com/index.html user_agent:
```

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #655 | Severity: High | Type: Data Exfiltration (Score: 21.0301)

Log Details:

syslog_ts: Jan 28 08:17:54 host: servernameabc process: httpd[12345] ip1: 10.132.39.84 ip2: 0.1.0.1 session_id: 27705 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:54 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 5625 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #659 | Severity: High | Type: Data Exfiltration (Score: 26.2297)

Log Details:

syslog_ts: Jan 28 08:17:58 host: servernameabc process: httpd[12345] ip1: 10.139.244.178 ip2: 0.1.0.1 session_id: 97684 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:58 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 15179 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #661 | Severity: High | Type: Data Exfiltration (Score: 16.8698)

Log Details:

syslog_ts: Jan 28 08:18:00 host: servernameabc process: httpd[12345] ip1: 10.184.122.147 ip2: 0.1.0.1 session_id: 23399 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:00 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 1449 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #663 | Severity: High | Type: Data Exfiltration (Score: 25.8156)

Log Details:

```
syslog_ts: Jan 28 08:18:01 host: servernameabc process: httpd[12345] ip1: 10.209.97.35 ip2: 0.1.0.1 session_id: 92451 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:01 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 13770 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #664 | Severity: High | Type: Data Exfiltration (Score: 26.1847)

Log Details:

```
syslog_ts: Jan 28 08:18:01 host: servernameabc process: httpd[12345] ip1: 10.62.213.53 ip2: 0.1.0.1 session_id: 74543 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:01 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 16560 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #666 | Severity: High | Type: Data Exfiltration (Score: 22.9158)

Log Details:

```
syslog_ts: Jan 28 08:18:02 host: servernameabc process: httpd[12345] ip1: 10.172.225.10 ip2: 0.1.0.1 session_id: 50915 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:02 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 7803 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #668 | Severity: High | Type: Data Exfiltration (Score: 27.1872)

Log Details:

```
syslog_ts: Jan 28 08:18:04 host: servernameabc process: httpd[12345] ip1: 10.12.113.120 ip2: 0.1.0.1 session_id: 89112 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:04 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 18894 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #669 | Severity: High | Type: Data Exfiltration (Score: 26.4705)

```
Log Details:
syslog_ts: Jan 28 08:18:05 host: servernameabc process: httpd[12345] ip1: 10.26.10.8 ip2: 0.1.0.1
session_id: 36442 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:05 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 13938 response_time: 46 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #671 | Severity: High | Type: Data Exfiltration (Score: 23.4183)

```
Log Details:
syslog_ts: Jan 28 08:18:06 host: servernameabc process: httpd[12345] ip1: 10.37.199.247 ip2: 0.1.0.1
session_id: 96570 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:06 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 9077 response_time: 25 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #673 | Severity: High | Type: Data Exfiltration (Score: 24.3649)

```
Log Details:
syslog_ts: Jan 28 08:18:06 host: servernameabc process: httpd[12345] ip1: 10.15.111.48 ip2: 0.1.0.1
session_id: 40422 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:06 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 10590 response_time: 29 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #674 | Severity: High | Type: Data Exfiltration (Score: 26.9539)

```
Log Details:
```

Anomaly Detection Report

syslog_ts: Jan 28 08:18:07 host: servernameabc process: httpd[12345] ip1: 10.90.36.146 ip2: 0.1.0.1 session_id: 96753 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:07 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 15416 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #677 | Severity: High | Type: Data Exfiltration (Score: 26.7984)

Log Details:

syslog_ts: Jan 28 08:18:10 host: servernameabc process: httpd[12345] ip1: 10.114.23.5 ip2: 0.1.0.1 session_id: 17974 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:10 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 19287 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #678 | Severity: High | Type: Data Exfiltration (Score: 21.8627)

Log Details:

syslog_ts: Jan 28 08:18:10 host: servernameabc process: httpd[12345] ip1: 10.210.200.160 ip2: 0.1.0.1 session_id: 79500 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:10 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 5991 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #679 | Severity: High | Type: Data Exfiltration (Score: 23.7919)

Log Details:

syslog_ts: Jan 28 08:18:11 host: servernameabc process: httpd[12345] ip1: 10.191.73.229 ip2: 0.1.0.1 session_id: 27969 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:11 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 8816 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #681 | Severity: High | Type: Data Exfiltration (Score: 17.1295)

Log Details:

```
syslog_ts: Jan 28 08:18:14 host: servernameabc process: httpd[12345] ip1: 10.115.44.72 ip2: 0.1.0.1 session_id: 26876 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:14 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 1787 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #682 | Severity: High | Type: Data Exfiltration (Score: 18.5336)

Log Details:

```
syslog_ts: Jan 28 08:18:14 host: servernameabc process: httpd[12345] ip1: 10.38.54.9 ip2: 0.1.0.1 session_id: 80752 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:14 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 3145 response_time: 20 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #683 | Severity: High | Type: Data Exfiltration (Score: 24.3872)

Log Details:

```
syslog_ts: Jan 28 08:18:15 host: servernameabc process: httpd[12345] ip1: 10.236.205.88 ip2: 0.1.0.1 session_id: 14484 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:15 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 16043 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #684 | Severity: High | Type: Data Exfiltration (Score: 23.2903)

Log Details:

```
syslog_ts: Jan 28 08:18:16 host: servernameabc process: httpd[12345] ip1: 10.222.230.145 ip2: 0.1.0.1 session_id: 11899 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:16 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 8373 response_time: 29 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #687 | Severity: High | Type: Data Exfiltration (Score: 15.9143)

Log Details:

syslog_ts: Jan 28 08:18:19 host: servernameabc process: httpd[12345] ip1: 10.0.218.28 ip2: 0.1.0.1 session_id: 83412 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:19 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 1282 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #688 | Severity: High | Type: Data Exfiltration (Score: 25.7032)

Log Details:

syslog_ts: Jan 28 08:18:20 host: servernameabc process: httpd[12345] ip1: 10.50.238.114 ip2: 0.1.0.1 session_id: 89411 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:20 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 12520 response_time: 40 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #690 | Severity: High | Type: Data Exfiltration (Score: 23.1016)

Log Details:

syslog_ts: Jan 28 08:18:21 host: servernameabc process: httpd[12345] ip1: 10.10.70.7 ip2: 0.1.0.1 session_id: 77303 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:21 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 11910 response_time: 7 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #691 | Severity: High | Type: Data Exfiltration (Score: 26.2852)

Log Details:

```
syslog_ts: Jan 28 08:18:22 host: servernameabc process: httpd[12345] ip1: 10.26.130.114 ip2: 0.1.0.1 session_id: 85352 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:22 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 16076 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #693 | Severity: High | Type: Data Exfiltration (Score: 19.0411)

Log Details:

```
syslog_ts: Jan 28 08:18:24 host: servernameabc process: httpd[12345] ip1: 10.126.86.12 ip2: 0.1.0.1 session_id: 73465 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:24 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 3844 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #694 | Severity: High | Type: Data Exfiltration (Score: 19.3028)

Log Details:

```
syslog_ts: Jan 28 08:18:25 host: servernameabc process: httpd[12345] ip1: 10.243.60.251 ip2: 0.1.0.1 session_id: 36124 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:25 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 3396 response_time: 27 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #695 | Severity: High | Type: Data Exfiltration (Score: 15.7310)

Log Details:

```
syslog_ts: Jan 28 08:18:25 host: servernameabc process: httpd[12345] ip1: 10.137.57.64 ip2: 0.1.0.1 session_id: 11986 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:25 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 1052 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #698 | Severity: High | Type: Data Exfiltration (Score: 22.7301)

```
Log Details:
syslog_ts: Jan 28 08:18:27 host: servernameabc process: httpd[12345] ip1: 10.253.114.224 ip2: 0.1.0.1 session_id: 89633 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:27 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 6878 response_time: 35 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #701 | Severity: High | Type: Data Exfiltration (Score: 27.1005)

```
Log Details:
syslog_ts: Jan 28 08:18:28 host: servernameabc process: httpd[12345] ip1: 10.135.22.251 ip2: 0.1.0.1 session_id: 45699 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:28 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 18564 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #702 | Severity: High | Type: Data Exfiltration (Score: 16.3883)

```
Log Details:
syslog_ts: Jan 28 08:18:30 host: servernameabc process: httpd[12345] ip1: 10.181.134.119 ip2: 0.1.0.1 session_id: 59196 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:30 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 1283 response_time: 43 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #705 | Severity: High | Type: Data Exfiltration (Score: 14.3664)

```
Log Details:
```

```
syslog_ts: Jan 28 08:18:33 host: servernameabc process: httpd[12345] ip1: 10.157.239.69 ip2: 0.1.0.1 session_id: 53557 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:33 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 1580 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #706 | Severity: High | Type: Data Exfiltration (Score: 26.4461)

Log Details:

```
syslog_ts: Jan 28 08:18:33 host: servernameabc process: httpd[12345] ip1: 10.124.18.242 ip2: 0.1.0.1 session_id: 37570 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:33 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 16052 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #708 | Severity: High | Type: Data Exfiltration (Score: 28.2127)

Log Details:

```
syslog_ts: Jan 28 08:18:34 host: servernameabc process: httpd[12345] ip1: 10.169.105.197 ip2: 0.1.0.1 session_id: 95589 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:34 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 19468 response_time: 49 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #711 | Severity: High | Type: Data Exfiltration (Score: 24.7530)

Log Details:

```
syslog_ts: Jan 28 08:18:37 host: servernameabc process: httpd[12345] ip1: 10.15.103.123 ip2: 0.1.0.1 session_id: 44268 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:37 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 14134 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #715 | Severity: High | Type: Data Exfiltration (Score: 26.3758)

Log Details:

```
syslog_ts: Jan 28 08:18:40 host: servernameabc process: httpd[12345] ip1: 10.102.34.17 ip2: 0.1.0.1 session_id: 60625 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:40 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 17697 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #719 | Severity: High | Type: Data Exfiltration (Score: 23.0586)

Log Details:

```
syslog_ts: Jan 28 08:18:44 host: servernameabc process: httpd[12345] ip1: 10.33.186.227 ip2: 0.1.0.1 session_id: 92887 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:44 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 7759 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #720 | Severity: High | Type: Data Exfiltration (Score: 24.3200)

Log Details:

```
syslog_ts: Jan 28 08:18:45 host: servernameabc process: httpd[12345] ip1: 10.3.3.185 ip2: 0.1.0.1 session_id: 36264 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:45 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 12456 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #722 | Severity: High | Type: Data Exfiltration (Score: 17.1059)

Log Details:

```
syslog_ts: Jan 28 08:18:46 host: servernameabc process: httpd[12345] ip1: 10.171.0.97 ip2: 0.1.0.1 session_id: 36460 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:46 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 2479 response_time: 14 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #723 | Severity: High | Type: Data Exfiltration (Score: 23.8674)

Log Details:

syslog_ts: Jan 28 08:18:47 host: servernameabc process: httpd[12345] ip1: 10.74.57.82 ip2: 0.1.0.1 session_id: 20045 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:47 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 14002 response_time: 7 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #725 | Severity: High | Type: Data Exfiltration (Score: 27.9255)

Log Details:

syslog_ts: Jan 28 08:18:49 host: servernameabc process: httpd[12345] ip1: 10.153.227.180 ip2: 0.1.0.1 session_id: 25505 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:49 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 19140 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #727 | Severity: High | Type: Data Exfiltration (Score: 25.5745)

Log Details:

syslog_ts: Jan 28 08:18:51 host: servernameabc process: httpd[12345] ip1: 10.160.185.124 ip2: 0.1.0.1 session_id: 31730 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:51 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 12811 response_time: 35 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #730 | Severity: High | Type: Data Exfiltration (Score: 25.8658)

Log Details:

syslog_ts: Jan 28 08:18:54 host: servernameabc process: httpd[12345] ip1: 10.24.49.181 ip2: 0.1.0.1 session_id: 45454 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:54 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 13767 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #732 | Severity: High | Type: Data Exfiltration (Score: 18.5490)

Log Details:

syslog_ts: Jan 28 08:18:56 host: servernameabc process: httpd[12345] ip1: 10.132.67.104 ip2: 0.1.0.1 session_id: 42269 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:56 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 2815 response_time: 27 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #733 | Severity: High | Type: Data Exfiltration (Score: 20.4370)

Log Details:

syslog_ts: Jan 28 08:18:57 host: servernameabc process: httpd[12345] ip1: 10.192.195.106 ip2: 0.1.0.1 session_id: 27700 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:57 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 3721 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #734 | Severity: High | Type: Data Exfiltration (Score: 26.4671)

Log Details:

syslog_ts: Jan 28 08:18:58 host: servernameabc process: httpd[12345] ip1: 10.162.116.145 ip2: 0.1.0.1 session_id: 81557 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:58 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 15444 response_time: 35 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #736 | Severity: High | Type: Data Exfiltration (Score: 21.8996)

Log Details:

syslog_ts: Jan 28 08:19:00 host: servernameabc process: httpd[12345] ip1: 10.130.190.127 ip2: 0.1.0.1 session_id: 28350 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:00 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 8935 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #737 | Severity: High | Type: Data Exfiltration (Score: 26.8489)

Log Details:

syslog_ts: Jan 28 08:19:00 host: servernameabc process: httpd[12345] ip1: 10.21.36.150 ip2: 0.1.0.1 session_id: 58489 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:00 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 15766 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #740 | Severity: High | Type: Data Exfiltration (Score: 17.6611)

Log Details:

syslog_ts: Jan 28 08:19:02 host: servernameabc process: httpd[12345] ip1: 10.181.82.71 ip2: 0.1.0.1 session_id: 83120 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:02 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 1977 response_time: 36 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #742 | Severity: High | Type: Data Exfiltration (Score: 10.4837)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:19:03 host: servernameabc process: httpd[12345] ip1: 10.124.156.161 ip2: 0.1.0.1
session_id: 82990 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:03 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 337 response_time: 16 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #744 | Severity: High | Type: Data Exfiltration (Score: 14.3771)

```
Log Details:
syslog_ts: Jan 28 08:19:04 host: servernameabc process: httpd[12345] ip1: 10.97.7.23 ip2: 0.1.0.1
session_id: 17866 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:04 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 1256 response_time: 12 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #745 | Severity: High | Type: Data Exfiltration (Score: 19.2901)

```
Log Details:
syslog_ts: Jan 28 08:19:05 host: servernameabc process: httpd[12345] ip1: 10.107.37.207 ip2: 0.1.0.1
session_id: 55549 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:05 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 3436 response_time: 26 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #747 | Severity: High | Type: Data Exfiltration (Score: 21.3705)

```
Log Details:
syslog_ts: Jan 28 08:19:06 host: servernameabc process: httpd[12345] ip1: 10.111.215.223 ip2: 0.1.0.1
session_id: 99280 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:06 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 5149 response_time: 33 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #749 | Severity: High | Type: Data Exfiltration (Score: 24.9175)

Log Details:

```
syslog_ts: Jan 28 08:19:07 host: servernameabc process: httpd[12345] ip1: 10.116.199.96 ip2: 0.1.0.1 session_id: 72895 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:07 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 10481 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #750 | Severity: High | Type: Data Exfiltration (Score: 26.4842)

Log Details:

```
syslog_ts: Jan 28 08:19:09 host: servernameabc process: httpd[12345] ip1: 10.170.122.212 ip2: 0.1.0.1 session_id: 23609 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:09 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 18350 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #751 | Severity: High | Type: Data Exfiltration (Score: 26.2352)

Log Details:

```
syslog_ts: Jan 28 08:19:09 host: servernameabc process: httpd[12345] ip1: 10.104.207.69 ip2: 0.1.0.1 session_id: 34231 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:09 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 19181 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #752 | Severity: High | Type: Data Exfiltration (Score: 27.6295)

Log Details:

```
syslog_ts: Jan 28 08:19:10 host: servernameabc process: httpd[12345] ip1: 10.123.1.218 ip2: 0.1.0.1 session_id: 24947 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:10 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 17150 response_time: 50 referer:
```

Anomaly Detection Report

```
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #753 | Severity: High | Type: Data Exfiltration (Score: 24.9581)

```
Log Details:
syslog_ts: Jan 28 08:19:12  host: servernameabc  process: httpd[12345]  ip1: 10.173.200.136  ip2: 0.1.0.1  session_id:  78540  domain:  abc.example.net  apache_ts:  28/Jan/2026:08:19:12  +0530  request:  GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1  status: 200  bytes: 11002  response_time: 37  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #754 | Severity: High | Type: Data Exfiltration (Score: 24.1853)

```
Log Details:
syslog_ts: Jan 28 08:19:13  host: servernameabc  process: httpd[12345]  ip1: 10.129.43.113  ip2: 0.1.0.1  session_id:  76178  domain:  abc.example.net  apache_ts:  28/Jan/2026:08:19:13  +0530  request:  GET /leave/appResources/images/lerf_default.png HTTP/1.1  status: 200  bytes: 9505  response_time: 35  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #756 | Severity: High | Type: Data Exfiltration (Score: 24.7557)

```
Log Details:
syslog_ts: Jan 28 08:19:15  host: servernameabc  process: httpd[12345]  ip1: 10.17.51.4  ip2: 0.1.0.1  session_id:  30101  domain:  abc.example.net  apache_ts:  28/Jan/2026:08:19:15  +0530  request:  GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1  status: 200  bytes: 9493  response_time: 48  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #762 | Severity: High | Type: Data Exfiltration (Score: 18.9725)

Log Details:

```
syslog_ts: Jan 28 08:19:18 host: servernameabc process: httpd[12345] ip1: 10.99.193.136 ip2: 0.1.0.1 session_id: 92342 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:18 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 2918 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #763 | Severity: High | Type: Data Exfiltration (Score: 23.7676)

Log Details:

```
syslog_ts: Jan 28 08:19:19 host: servernameabc process: httpd[12345] ip1: 10.1.121.92 ip2: 0.1.0.1 session_id: 36697 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:19 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 9666 response_time: 26 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #765 | Severity: High | Type: Data Exfiltration (Score: 22.0679)

Log Details:

```
syslog_ts: Jan 28 08:19:20 host: servernameabc process: httpd[12345] ip1: 10.106.239.24 ip2: 0.1.0.1 session_id: 27607 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:20 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 10125 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #767 | Severity: High | Type: Data Exfiltration (Score: 26.6983)

Log Details:

```
syslog_ts: Jan 28 08:19:21 host: servernameabc process: httpd[12345] ip1: 10.76.235.51 ip2: 0.1.0.1 session_id: 59168 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:21 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 14618 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #769 | Severity: High | Type: Data Exfiltration (Score: 19.7210)

```
Log Details:
syslog_ts: Jan 28 08:19:22 host: servernameabc process: httpd[12345] ip1: 10.18.6.219 ip2: 0.1.0.1 session_id: 65761 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:22 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 3468 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #770 | Severity: High | Type: Data Exfiltration (Score: 20.5098)

```
Log Details:
syslog_ts: Jan 28 08:19:22 host: servernameabc process: httpd[12345] ip1: 10.49.184.17 ip2: 0.1.0.1 session_id: 16468 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:22 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 3496 response_time: 50 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #771 | Severity: High | Type: Data Exfiltration (Score: 25.7916)

```
Log Details:
syslog_ts: Jan 28 08:19:22 host: servernameabc process: httpd[12345] ip1: 10.9.2.198 ip2: 0.1.0.1 session_id: 57040 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:22 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 13273 response_time: 36 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #772 | Severity: High | Type: Data Exfiltration (Score: 25.8018)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:19:23 host: servernameabc process: httpd[12345] ip1: 10.142.166.18 ip2: 0.1.0.1 session_id: 99248 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:23 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 18220 response_time: 13 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #775 | Severity: High | Type: Data Exfiltration (Score: 16.7433)

```
Log Details:
syslog_ts: Jan 28 08:19:25 host: servernameabc process: httpd[12345] ip1: 10.247.252.67 ip2: 0.1.0.1 session_id: 72589 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:25 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 2258 response_time: 14 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #777 | Severity: High | Type: Data Exfiltration (Score: 23.6454)

```
Log Details:
syslog_ts: Jan 28 08:19:27 host: servernameabc process: httpd[12345] ip1: 10.196.202.31 ip2: 0.1.0.1 session_id: 70700 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:27 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 7630 response_time: 45 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #778 | Severity: High | Type: Data Exfiltration (Score: 22.6741)

```
Log Details:
syslog_ts: Jan 28 08:19:28 host: servernameabc process: httpd[12345] ip1: 10.25.32.162 ip2: 0.1.0.1 session_id: 36426 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:28 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 7206 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #779 | Severity: High | Type: Data Exfiltration (Score: 24.3279)

Log Details:

```
syslog_ts: Jan 28 08:19:28 host: servernameabc process: httpd[12345] ip1: 10.119.170.72 ip2: 0.1.0.1 session_id: 51226 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:28 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 11059 response_time: 25 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #785 | Severity: High | Type: Data Exfiltration (Score: 25.6703)

Log Details:

```
syslog_ts: Jan 28 08:19:32 host: servernameabc process: httpd[12345] ip1: 10.235.166.130 ip2: 0.1.0.1 session_id: 70150 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:32 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 12200 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #786 | Severity: High | Type: Data Exfiltration (Score: 18.4591)

Log Details:

```
syslog_ts: Jan 28 08:19:33 host: servernameabc process: httpd[12345] ip1: 10.238.6.15 ip2: 0.1.0.1 session_id: 25174 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:33 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 2598 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #787 | Severity: High | Type: Data Exfiltration (Score: 26.9159)

Log Details:

```
syslog_ts: Jan 28 08:19:35 host: servernameabc process: httpd[12345] ip1: 10.229.238.196 ip2: 0.1.0.1 session_id: 30618 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:35 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 18084 response_time: 29 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #788 | Severity: High | Type: Data Exfiltration (Score: 21.5003)

Log Details:

syslog_ts: Jan 28 08:19:35 host: servernameabc process: httpd[12345] ip1: 10.130.188.246 ip2: 0.1.0.1 session_id: 79839 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:35 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 8412 response_time: 7 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #790 | Severity: High | Type: Data Exfiltration (Score: 26.4617)

Log Details:

syslog_ts: Jan 28 08:19:37 host: servernameabc process: httpd[12345] ip1: 10.18.132.103 ip2: 0.1.0.1 session_id: 83880 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:37 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 14284 response_time: 43 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #791 | Severity: High | Type: Data Exfiltration (Score: 27.2530)

Log Details:

syslog_ts: Jan 28 08:19:37 host: servernameabc process: httpd[12345] ip1: 10.56.81.192 ip2: 0.1.0.1 session_id: 54856 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:37 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 18340 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #794 | Severity: High | Type: Data Exfiltration (Score: 12.9847)

Log Details:

```
syslog_ts: Jan 28 08:19:41 host: servernameabc process: httpd[12345] ip1: 10.153.226.52 ip2: 0.1.0.1 session_id: 75130 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:41 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 595 response_time: 27 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #795 | Severity: High | Type: Data Exfiltration (Score: 22.4433)

Log Details:

```
syslog_ts: Jan 28 08:19:42 host: servernameabc process: httpd[12345] ip1: 10.82.145.244 ip2: 0.1.0.1 session_id: 91947 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:42 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 7524 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #797 | Severity: High | Type: Data Exfiltration (Score: 25.5236)

Log Details:

```
syslog_ts: Jan 28 08:19:43 host: servernameabc process: httpd[12345] ip1: 10.3.14.165 ip2: 0.1.0.1 session_id: 98504 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:43 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 11115 response_time: 49 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #799 | Severity: High | Type: Data Exfiltration (Score: 24.0601)

Log Details:

```
syslog_ts: Jan 28 08:19:45 host: servernameabc process: httpd[12345] ip1: 10.93.105.122 ip2: 0.1.0.1 session_id: 13185 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:45 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 14199 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #800 | Severity: High | Type: Data Exfiltration (Score: 24.3341)

```
Log Details:
syslog_ts: Jan 28 08:19:45 host: servernameabc process: httpd[12345] ip1: 10.197.130.57 ip2: 0.1.0.1 session_id: 45287 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:45 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 16347 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #805 | Severity: High | Type: Data Exfiltration (Score: 27.7875)

```
Log Details:
syslog_ts: Jan 28 08:19:50 host: servernameabc process: httpd[12345] ip1: 10.117.198.206 ip2: 0.1.0.1 session_id: 12992 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:50 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 18298 response_time: 46 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #806 | Severity: High | Type: Data Exfiltration (Score: 24.8496)

```
Log Details:
syslog_ts: Jan 28 08:19:50 host: servernameabc process: httpd[12345] ip1: 10.245.59.158 ip2: 0.1.0.1 session_id: 35388 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:50 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 10041 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #807 | Severity: High | Type: Data Exfiltration (Score: 26.3528)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:19:50 host: servernameabc process: httpd[12345] ip1: 10.70.69.191 ip2: 0.1.0.1
session_id: 41259 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:50 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 13598 response_time: 46 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #809 | Severity: High | Type: Data Exfiltration (Score: 23.0534)

```
Log Details:
syslog_ts: Jan 28 08:19:52 host: servernameabc process: httpd[12345] ip1: 10.85.23.49 ip2: 0.1.0.1
session_id: 52193 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:52 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 9322 response_time: 18 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #810 | Severity: High | Type: Data Exfiltration (Score: 25.5128)

```
Log Details:
syslog_ts: Jan 28 08:19:53 host: servernameabc process: httpd[12345] ip1: 10.122.14.43 ip2: 0.1.0.1
session_id: 71398 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:53 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 15989 response_time: 17 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #811 | Severity: High | Type: Data Exfiltration (Score: 24.9873)

```
Log Details:
syslog_ts: Jan 28 08:19:54 host: servernameabc process: httpd[12345] ip1: 10.11.112.24 ip2: 0.1.0.1
session_id: 30618 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:54 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 18686 response_time: 5 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #815 | Severity: High | Type: Data Exfiltration (Score: 26.5205)

Log Details:

```
syslog_ts: Jan 28 08:19:57 host: servernameabc process: httpd[12345] ip1: 10.245.68.27 ip2: 0.1.0.1 session_id: 50306 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:57 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 19336 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #817 | Severity: High | Type: Data Exfiltration (Score: 22.6557)

Log Details:

```
syslog_ts: Jan 28 08:19:58 host: servernameabc process: httpd[12345] ip1: 10.158.208.210 ip2: 0.1.0.1 session_id: 62068 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:58 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 9580 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #818 | Severity: High | Type: Data Exfiltration (Score: 17.7731)

Log Details:

```
syslog_ts: Jan 28 08:19:59 host: servernameabc process: httpd[12345] ip1: 10.200.211.83 ip2: 0.1.0.1 session_id: 84528 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:59 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 3785 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #819 | Severity: High | Type: Data Exfiltration (Score: 24.7797)

Log Details:

```
syslog_ts: Jan 28 08:20:00 host: servernameabc process: httpd[12345] ip1: 10.193.221.235 ip2: 0.1.0.1 session_id: 37231 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:00 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 9461 response_time: 49 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #820 | Severity: High | Type: Data Exfiltration (Score: 15.7554)

Log Details:

syslog_ts: Jan 28 08:20:02 host: servernameabc process: httpd[12345] ip1: 10.16.40.101 ip2: 0.1.0.1 session_id: 47937 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:02 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 1392 response_time: 25 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #821 | Severity: High | Type: Data Exfiltration (Score: 22.9522)

Log Details:

syslog_ts: Jan 28 08:20:03 host: servernameabc process: httpd[12345] ip1: 10.251.79.103 ip2: 0.1.0.1 session_id: 10580 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:03 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 10218 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #823 | Severity: High | Type: Data Exfiltration (Score: 24.4290)

Log Details:

syslog_ts: Jan 28 08:20:04 host: servernameabc process: httpd[12345] ip1: 10.32.160.113 ip2: 0.1.0.1 session_id: 42164 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:04 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 12536 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #825 | Severity: High | Type: Data Exfiltration (Score: 25.8570)

Log Details:

```
syslog_ts: Jan 28 08:20:06 host: servernameabc process: httpd[12345] ip1: 10.94.121.13 ip2: 0.1.0.1 session_id: 10376 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:06 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 17163 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #826 | Severity: High | Type: Data Exfiltration (Score: 20.5842)

Log Details:

```
syslog_ts: Jan 28 08:20:07 host: servernameabc process: httpd[12345] ip1: 10.170.76.159 ip2: 0.1.0.1 session_id: 90287 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:07 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 4029 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #827 | Severity: High | Type: Data Exfiltration (Score: 25.3525)

Log Details:

```
syslog_ts: Jan 28 08:20:08 host: servernameabc process: httpd[12345] ip1: 10.71.179.49 ip2: 0.1.0.1 session_id: 87644 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:08 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 12772 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #828 | Severity: High | Type: Data Exfiltration (Score: 21.6902)

Log Details:

```
syslog_ts: Jan 28 08:20:08 host: servernameabc process: httpd[12345] ip1: 10.207.27.75 ip2: 0.1.0.1 session_id: 53166 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:08 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 8107 response_time: 10 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #829 | Severity: High | Type: Data Exfiltration (Score: 26.3490)

```
Log Details:
syslog_ts: Jan 28 08:20:08 host: servernameabc process: httpd[12345] ip1: 10.213.226.66 ip2: 0.1.0.1
session_id: 36095 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:08 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 15733 response_time: 31 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #830 | Severity: High | Type: Data Exfiltration (Score: 27.6509)

```
Log Details:
syslog_ts: Jan 28 08:20:09 host: servernameabc process: httpd[12345] ip1: 10.45.87.168 ip2: 0.1.0.1
session_id: 69965 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:09 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 17795 response_time: 46 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #835 | Severity: High | Type: Data Exfiltration (Score: 24.8276)

```
Log Details:
syslog_ts: Jan 28 08:20:12 host: servernameabc process: httpd[12345] ip1: 10.76.184.172 ip2: 0.1.0.1
session_id: 93769 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:12 +0530 request: GET
/leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 9814 response_time: 46 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #837 | Severity: High | Type: Data Exfiltration (Score: 14.2877)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:20:13 host: servernameabc process: httpd[12345] ip1: 10.232.87.213 ip2: 0.1.0.1
session_id: 13743 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:13 +0530 request: GET /favicon.ico
HTTP/1.1 status: 200 bytes: 1192 response_time: 13 referer: https://abc.example.com/index.html user_agent:
Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0
Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #840 | Severity: High | Type: Data Exfiltration (Score: 27.5771)

```
Log Details:
syslog_ts: Jan 28 08:20:15 host: servernameabc process: httpd[12345] ip1: 10.153.59.226 ip2: 0.1.0.1
session_id: 97660 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:15 +0530 request: GET /favicon.ico
HTTP/1.1 status: 200 bytes: 18827 response_time: 38 referer: https://abc.example.com/index.html
user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0
Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #843 | Severity: High | Type: Data Exfiltration (Score: 25.8024)

```
Log Details:
syslog_ts: Jan 28 08:20:18 host: servernameabc process: httpd[12345] ip1: 10.94.185.5 ip2: 0.1.0.1
session_id: 46491 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:18 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 16439 response_time: 19 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #846 | Severity: High | Type: Data Exfiltration (Score: 22.8722)

```
Log Details:
syslog_ts: Jan 28 08:20:19 host: servernameabc process: httpd[12345] ip1: 10.61.22.242 ip2: 0.1.0.1
session_id: 36753 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:19 +0530 request: GET /favicon.ico
HTTP/1.1 status: 200 bytes: 7629 response_time: 29 referer: https://abc.example.com/index.html user_agent:
Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0
Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #848 | Severity: High | Type: Data Exfiltration (Score: 23.2356)

Log Details:

```
syslog_ts: Jan 28 08:20:21 host: servernameabc process: httpd[12345] ip1: 10.117.214.183 ip2: 0.1.0.1 session_id: 57279 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:21 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 8378 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #849 | Severity: High | Type: Data Exfiltration (Score: 24.0798)

Log Details:

```
syslog_ts: Jan 28 08:20:22 host: servernameabc process: httpd[12345] ip1: 10.244.89.7 ip2: 0.1.0.1 session_id: 78837 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:22 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 10210 response_time: 27 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #850 | Severity: High | Type: Data Exfiltration (Score: 25.6413)

Log Details:

```
syslog_ts: Jan 28 08:20:24 host: servernameabc process: httpd[12345] ip1: 10.67.140.75 ip2: 0.1.0.1 session_id: 68836 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:24 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 13731 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #851 | Severity: High | Type: Data Exfiltration (Score: 16.6369)

Log Details:

```
syslog_ts: Jan 28 08:20:24 host: servernameabc process: httpd[12345] ip1: 10.181.175.64 ip2: 0.1.0.1 session_id: 75171 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:24 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 2433 response_time: 10 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #852 | Severity: High | Type: Data Exfiltration (Score: 24.7416)

Log Details:

syslog_ts: Jan 28 08:20:24 host: servernameabc process: httpd[12345] ip1: 10.148.37.221 ip2: 0.1.0.1 session_id: 28609 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:24 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 11483 response_time: 29 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #853 | Severity: High | Type: Data Exfiltration (Score: 23.3016)

Log Details:

syslog_ts: Jan 28 08:20:25 host: servernameabc process: httpd[12345] ip1: 10.90.236.46 ip2: 0.1.0.1 session_id: 33656 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:25 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 10792 response_time: 13 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #854 | Severity: High | Type: Data Exfiltration (Score: 26.8456)

Log Details:

syslog_ts: Jan 28 08:20:25 host: servernameabc process: httpd[12345] ip1: 10.48.20.143 ip2: 0.1.0.1 session_id: 32970 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:25 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 17826 response_time: 29 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #855 | Severity: High | Type: Data Exfiltration (Score: 20.4026)

Log Details:

```
syslog_ts: Jan 28 08:20:27 host: servernameabc process: httpd[12345] ip1: 10.155.11.195 ip2: 0.1.0.1 session_id: 19043 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:27 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 5419 response_time: 15 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #857 | Severity: High | Type: Data Exfiltration (Score: 23.9426)

Log Details:

```
syslog_ts: Jan 28 08:20:28 host: servernameabc process: httpd[12345] ip1: 10.41.50.71 ip2: 0.1.0.1 session_id: 89664 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:28 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 11494 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #858 | Severity: High | Type: Data Exfiltration (Score: 12.8707)

Log Details:

```
syslog_ts: Jan 28 08:20:29 host: servernameabc process: httpd[12345] ip1: 10.124.104.197 ip2: 0.1.0.1 session_id: 95108 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:29 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 621 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #859 | Severity: High | Type: Data Exfiltration (Score: 17.4107)

Log Details:

```
syslog_ts: Jan 28 08:20:30 host: servernameabc process: httpd[12345] ip1: 10.242.5.76 ip2: 0.1.0.1 session_id: 76401 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:30 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 2170 response_time: 25 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #860 | Severity: High | Type: Data Exfiltration (Score: 20.6021)

```
Log Details:
syslog_ts: Jan 28 08:20:31 host: servernameabc process: httpd[12345] ip1: 10.234.108.243 ip2: 0.1.0.1 session_id: 85189 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:31 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 5793 response_time: 14 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #861 | Severity: High | Type: Data Exfiltration (Score: 24.6411)

```
Log Details:
syslog_ts: Jan 28 08:20:31 host: servernameabc process: httpd[12345] ip1: 10.198.191.53 ip2: 0.1.0.1 session_id: 83442 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:31 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 9258 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #862 | Severity: High | Type: Data Exfiltration (Score: 25.2970)

```
Log Details:
syslog_ts: Jan 28 08:20:31 host: servernameabc process: httpd[12345] ip1: 10.218.118.246 ip2: 0.1.0.1 session_id: 86082 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:31 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 12770 response_time: 30 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #863 | Severity: High | Type: Data Exfiltration (Score: 23.8807)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:20:32 host: servernameabc process: httpd[12345] ip1: 10.118.13.236 ip2: 0.1.0.1 session_id: 14734 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:32 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 9197 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #864 | Severity: High | Type: Data Exfiltration (Score: 22.7321)

Log Details:

```
syslog_ts: Jan 28 08:20:33 host: servernameabc process: httpd[12345] ip1: 10.242.62.66 ip2: 0.1.0.1 session_id: 44799 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:33 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 7041 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #866 | Severity: High | Type: Data Exfiltration (Score: 27.7579)

Log Details:

```
syslog_ts: Jan 28 08:20:34 host: servernameabc process: httpd[12345] ip1: 10.87.0.46 ip2: 0.1.0.1 session_id: 38494 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:34 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 18995 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #867 | Severity: High | Type: Data Exfiltration (Score: 25.7654)

Log Details:

```
syslog_ts: Jan 28 08:20:36 host: servernameabc process: httpd[12345] ip1: 10.205.14.132 ip2: 0.1.0.1 session_id: 28196 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:36 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 15392 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #871 | Severity: High | Type: Data Exfiltration (Score: 22.3951)

Log Details:

```
syslog_ts: Jan 28 08:20:40 host: servernameabc process: httpd[12345] ip1: 10.172.104.136 ip2: 0.1.0.1 session_id: 39768 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:40 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 8062 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #872 | Severity: High | Type: Data Exfiltration (Score: 23.2800)

Log Details:

```
syslog_ts: Jan 28 08:20:41 host: servernameabc process: httpd[12345] ip1: 10.120.98.45 ip2: 0.1.0.1 session_id: 16703 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:41 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 7234 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #873 | Severity: High | Type: Data Exfiltration (Score: 18.7899)

Log Details:

```
syslog_ts: Jan 28 08:20:41 host: servernameabc process: httpd[12345] ip1: 10.186.234.74 ip2: 0.1.0.1 session_id: 50403 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:41 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 3132 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #874 | Severity: High | Type: Data Exfiltration (Score: 25.5428)

Log Details:

```
syslog_ts: Jan 28 08:20:42 host: servernameabc process: httpd[12345] ip1: 10.124.119.116 ip2: 0.1.0.1 session_id: 66290 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:42 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 17625 response_time: 12 referer: https://abc.example.com/index.html
```

user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #875 | Severity: High | Type: Data Exfiltration (Score: 16.6044)

Log Details:

syslog_ts: Jan 28 08:20:43 host: servernameabc process: httpd[12345] ip1: 10.1.146.170 ip2: 0.1.0.1 session_id: 69231 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:43 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 2178 response_time: 14 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #876 | Severity: High | Type: Data Exfiltration (Score: 24.7623)

Log Details:

syslog_ts: Jan 28 08:20:43 host: servernameabc process: httpd[12345] ip1: 10.19.10.230 ip2: 0.1.0.1 session_id: 44939 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:43 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 13450 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #878 | Severity: High | Type: Data Exfiltration (Score: 25.2930)

Log Details:

syslog_ts: Jan 28 08:20:45 host: servernameabc process: httpd[12345] ip1: 10.7.221.27 ip2: 0.1.0.1 session_id: 36960 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:45 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 13948 response_time: 23 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #879 | Severity: High | Type: Data Exfiltration (Score: 26.3727)

Log Details:

```
syslog_ts: Jan 28 08:20:45 host: servernameabc process: httpd[12345] ip1: 10.124.95.209 ip2: 0.1.0.1 session_id: 50446 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:45 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 16775 response_time: 26 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #880 | Severity: High | Type: Data Exfiltration (Score: 22.6005)

Log Details:

```
syslog_ts: Jan 28 08:20:47 host: servernameabc process: httpd[12345] ip1: 10.38.33.195 ip2: 0.1.0.1 session_id: 70246 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:47 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 11011 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #881 | Severity: High | Type: Data Exfiltration (Score: 26.8177)

Log Details:

```
syslog_ts: Jan 28 08:20:47 host: servernameabc process: httpd[12345] ip1: 10.64.113.143 ip2: 0.1.0.1 session_id: 51356 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:47 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 15811 response_time: 40 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #882 | Severity: High | Type: Data Exfiltration (Score: 24.2497)

Log Details:

```
syslog_ts: Jan 28 08:20:48 host: servernameabc process: httpd[12345] ip1: 10.83.234.109 ip2: 0.1.0.1 session_id: 50983 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:48 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 9968 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #883 | Severity: High | Type: Data Exfiltration (Score: 20.0943)

```
Log Details:
syslog_ts: Jan 28 08:20:49 host: servernameabc process: httpd[12345] ip1: 10.76.92.234 ip2: 0.1.0.1
session_id: 66324 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:49 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 4059 response_time: 28 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #884 | Severity: High | Type: Data Exfiltration (Score: 18.1607)

```
Log Details:
syslog_ts: Jan 28 08:20:50 host: servernameabc process: httpd[12345] ip1: 10.199.69.169 ip2: 0.1.0.1
session_id: 10339 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:50 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 2005 response_time: 46 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #885 | Severity: High | Type: Data Exfiltration (Score: 17.1468)

```
Log Details:
syslog_ts: Jan 28 08:20:51 host: servernameabc process: httpd[12345] ip1: 10.89.87.176 ip2: 0.1.0.1
session_id: 74183 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:51 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 1600 response_time: 42 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #888 | Severity: High | Type: Data Exfiltration (Score: 21.8474)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:20:53 host: servernameabc process: httpd[12345] ip1: 10.139.157.24 ip2: 0.1.0.1 session_id: 66595 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:53 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 7010 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #889 | Severity: High | Type: Data Exfiltration (Score: 24.8939)

Log Details:

```
syslog_ts: Jan 28 08:20:53 host: servernameabc process: httpd[12345] ip1: 10.212.159.222 ip2: 0.1.0.1 session_id: 79440 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:53 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 10138 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #890 | Severity: High | Type: Data Exfiltration (Score: 10.7355)

Log Details:

```
syslog_ts: Jan 28 08:20:53 host: servernameabc process: httpd[12345] ip1: 10.46.110.85 ip2: 0.1.0.1 session_id: 26195 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:53 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 224 response_time: 39 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #891 | Severity: High | Type: Data Exfiltration (Score: 19.0335)

Log Details:

```
syslog_ts: Jan 28 08:20:54 host: servernameabc process: httpd[12345] ip1: 10.1.131.46 ip2: 0.1.0.1 session_id: 51996 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:54 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 4942 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #894 | Severity: High | Type: Data Exfiltration (Score: 22.2530)

Log Details:

```
syslog_ts: Jan 28 08:20:55 host: servernameabc process: httpd[12345] ip1: 10.183.216.225 ip2: 0.1.0.1
session_id: 10065 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:55 +0530 request: GET /favicon.ico
HTTP/1.1 status: 200 bytes: 5782 response_time: 41 referer: https://abc.example.com/index.html user_agent:
Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #895 | Severity: High | Type: Data Exfiltration (Score: 17.6797)

Log Details:

```
syslog_ts: Jan 28 08:20:55 host: servernameabc process: httpd[12345] ip1: 10.240.236.109 ip2: 0.1.0.1
session_id: 52958 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:55 +0530 request: GET /favicon.ico
HTTP/1.1 status: 200 bytes: 1691 response_time: 50 referer: https://abc.example.com/index.html user_agent:
Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #897 | Severity: High | Type: Data Exfiltration (Score: 21.0466)

Log Details:

```
syslog_ts: Jan 28 08:20:56 host: servernameabc process: httpd[12345] ip1: 10.232.148.125 ip2: 0.1.0.1
session_id: 24570 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:56 +0530 request: GET /favicon.ico
HTTP/1.1 status: 200 bytes: 5233 response_time: 26 referer: https://abc.example.com/index.html user_agent:
Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0
Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #898 | Severity: High | Type: Data Exfiltration (Score: 27.1285)

Log Details:

```
syslog_ts: Jan 28 08:20:57 host: servernameabc process: httpd[12345] ip1: 10.96.47.95 ip2: 0.1.0.1
session_id: 78790 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:57 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 17880 response_time: 34 referer:
```

```
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #899 | Severity: High | Type: Data Exfiltration (Score: 20.5140)

```
Log Details:
syslog_ts: Jan 28 08:20:57  host: servernameabc  process: httpd[12345]  ip1: 10.107.208.126  ip2: 0.1.0.1  session_id: 13028  domain: abc.example.net  apache_ts: 28/Jan/2026:08:20:57 +0530  request: GET /leave/appResources/images/lerf_default.png HTTP/1.1  status: 200  bytes: 4551  response_time: 27  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #903 | Severity: High | Type: Data Exfiltration (Score: 27.1173)

```
Log Details:
syslog_ts: Jan 28 08:21:00  host: servernameabc  process: httpd[12345]  ip1: 10.110.80.103  ip2: 0.1.0.1  session_id: 35224  domain: abc.example.net  apache_ts: 28/Jan/2026:08:21:00 +0530  request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1  status: 200  bytes: 17657  response_time: 35  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #904 | Severity: High | Type: Data Exfiltration (Score: 20.3963)

```
Log Details:
syslog_ts: Jan 28 08:21:01  host: servernameabc  process: httpd[12345]  ip1: 10.48.47.47  ip2: 0.1.0.1  session_id: 57616  domain: abc.example.net  apache_ts: 28/Jan/2026:08:21:01 +0530  request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1  status: 200  bytes: 3571  response_time: 45  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #907 | Severity: High | Type: Data Exfiltration (Score: 26.4376)

Log Details:

```
syslog_ts: Jan 28 08:21:04 host: servernameabc process: httpd[12345] ip1: 10.251.149.131 ip2: 0.1.0.1 session_id: 45025 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:04 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 17443 response_time: 24 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #908 | Severity: High | Type: Data Exfiltration (Score: 19.9013)

Log Details:

```
syslog_ts: Jan 28 08:21:05 host: servernameabc process: httpd[12345] ip1: 10.146.104.142 ip2: 0.1.0.1 session_id: 20726 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:05 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 3228 response_time: 43 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #909 | Severity: High | Type: Data Exfiltration (Score: 26.4281)

Log Details:

```
syslog_ts: Jan 28 08:21:05 host: servernameabc process: httpd[12345] ip1: 10.14.1.227 ip2: 0.1.0.1 session_id: 96082 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:05 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 15480 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #910 | Severity: High | Type: Data Exfiltration (Score: 27.7379)

Log Details:

```
syslog_ts: Jan 28 08:21:05 host: servernameabc process: httpd[12345] ip1: 10.20.162.221 ip2: 0.1.0.1 session_id: 60723 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:05 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 18749 response_time: 42 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #913 | Severity: High | Type: Data Exfiltration (Score: 23.3981)

```
Log Details:
syslog_ts: Jan 28 08:21:08 host: servernameabc process: httpd[12345] ip1: 10.164.11.134 ip2: 0.1.0.1 session_id: 24982 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:08 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 8575 response_time: 29 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #914 | Severity: High | Type: Data Exfiltration (Score: 20.7878)

```
Log Details:
syslog_ts: Jan 28 08:21:09 host: servernameabc process: httpd[12345] ip1: 10.108.105.195 ip2: 0.1.0.1 session_id: 40200 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:09 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 3777 response_time: 49 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #915 | Severity: High | Type: Data Exfiltration (Score: 23.8559)

```
Log Details:
syslog_ts: Jan 28 08:21:09 host: servernameabc process: httpd[12345] ip1: 10.148.177.37 ip2: 0.1.0.1 session_id: 84741 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:09 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 9255 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #917 | Severity: High | Type: Data Exfiltration (Score: 21.4768)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:21:12 host: servernameabc process: httpd[12345] ip1: 10.97.70.60 ip2: 0.1.0.1 session_id: 40918 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:12 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 6801 response_time: 16 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #922 | Severity: High | Type: Data Exfiltration (Score: 27.4224)

Log Details:

```
syslog_ts: Jan 28 08:21:16 host: servernameabc process: httpd[12345] ip1: 10.125.59.145 ip2: 0.1.0.1 session_id: 89766 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:16 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 17740 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #923 | Severity: High | Type: Data Exfiltration (Score: 21.4965)

Log Details:

```
syslog_ts: Jan 28 08:21:17 host: servernameabc process: httpd[12345] ip1: 10.69.234.32 ip2: 0.1.0.1 session_id: 21150 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:17 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 5119 response_time: 36 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #926 | Severity: High | Type: Data Exfiltration (Score: 21.5908)

Log Details:

```
syslog_ts: Jan 28 08:21:19 host: servernameabc process: httpd[12345] ip1: 10.40.207.63 ip2: 0.1.0.1 session_id: 44395 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:19 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 6614 response_time: 19 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #928 | Severity: High | Type: Data Exfiltration (Score: 26.9378)

Log Details:

```
syslog_ts: Jan 28 08:21:21 host: servernameabc process: httpd[12345] ip1: 10.106.111.194 ip2: 0.1.0.1 session_id: 71419 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:21 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 19839 response_time: 22 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #931 | Severity: High | Type: Data Exfiltration (Score: 17.6116)

Log Details:

```
syslog_ts: Jan 28 08:21:24 host: servernameabc process: httpd[12345] ip1: 10.101.188.99 ip2: 0.1.0.1 session_id: 44751 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:24 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 3200 response_time: 9 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #935 | Severity: High | Type: Data Exfiltration (Score: 19.5307)

Log Details:

```
syslog_ts: Jan 28 08:21:26 host: servernameabc process: httpd[12345] ip1: 10.251.241.225 ip2: 0.1.0.1 session_id: 13878 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:26 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 3188 response_time: 36 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #936 | Severity: High | Type: Data Exfiltration (Score: 25.9683)

Log Details:

```
syslog_ts: Jan 28 08:21:27 host: servernameabc process: httpd[12345] ip1: 10.103.108.218 ip2: 0.1.0.1 session_id: 74378 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:27 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 17559 response_time: 17
```

referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #937 | Severity: High | Type: Data Exfiltration (Score: 17.1635)

Log Details:

syslog_ts: Jan 28 08:21:28 host: servernameabc process: httpd[12345] ip1: 10.17.64.252 ip2: 0.1.0.1 session_id: 41985 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:28 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 2221 response_time: 20 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #938 | Severity: High | Type: Data Exfiltration (Score: 24.6561)

Log Details:

syslog_ts: Jan 28 08:21:28 host: servernameabc process: httpd[12345] ip1: 10.151.144.223 ip2: 0.1.0.1 session_id: 15110 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:28 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 13373 response_time: 17 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #939 | Severity: High | Type: Data Exfiltration (Score: 22.6120)

Log Details:

syslog_ts: Jan 28 08:21:29 host: servernameabc process: httpd[12345] ip1: 10.41.163.104 ip2: 0.1.0.1 session_id: 65462 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:29 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 8183 response_time: 20 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #940 | Severity: High | Type: Data Exfiltration (Score: 22.3041)

Log Details:

```
syslog_ts: Jan 28 08:21:30 host: servernameabc process: httpd[12345] ip1: 10.206.7.186 ip2: 0.1.0.1 session_id: 39806 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:30 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 6389 response_time: 33 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #941 | Severity: High | Type: Data Exfiltration (Score: 16.7690)

Log Details:

```
syslog_ts: Jan 28 08:21:30 host: servernameabc process: httpd[12345] ip1: 10.255.155.92 ip2: 0.1.0.1 session_id: 43204 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:30 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 1645 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #942 | Severity: High | Type: Data Exfiltration (Score: 26.4740)

Log Details:

```
syslog_ts: Jan 28 08:21:32 host: servernameabc process: httpd[12345] ip1: 10.152.180.11 ip2: 0.1.0.1 session_id: 25675 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:32 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 15466 response_time: 35 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #944 | Severity: High | Type: Data Exfiltration (Score: 21.1418)

Log Details:

```
syslog_ts: Jan 28 08:21:33 host: servernameabc process: httpd[12345] ip1: 10.142.240.97 ip2: 0.1.0.1 session_id: 28215 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:33 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 7552 response_time: 8 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #946 | Severity: High | Type: Data Exfiltration (Score: 20.0743)

```
Log Details:
syslog_ts: Jan 28 08:21:35 host: servernameabc process: httpd[12345] ip1: 10.82.85.23 ip2: 0.1.0.1
session_id: 76080 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:35 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 3984 response_time: 29 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #947 | Severity: High | Type: Data Exfiltration (Score: 24.8874)

```
Log Details:
syslog_ts: Jan 28 08:21:35 host: servernameabc process: httpd[12345] ip1: 10.170.161.189 ip2: 0.1.0.1
session_id: 64059 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:35 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 9855 response_time: 47 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #949 | Severity: High | Type: Data Exfiltration (Score: 16.8990)

```
Log Details:
syslog_ts: Jan 28 08:21:37 host: servernameabc process: httpd[12345] ip1: 10.87.207.186 ip2: 0.1.0.1
session_id: 26799 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:37 +0530 request: GET
/timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 2847 response_time: 7 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #950 | Severity: High | Type: Data Exfiltration (Score: 13.6221)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:21:37 host: servernameabc process: httpd[12345] ip1: 10.72.87.90 ip2: 0.1.0.1
session_id: 92733 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:37 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 1013 response_time: 12 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #951 | Severity: High | Type: Data Exfiltration (Score: 10.6703)

```
Log Details:
syslog_ts: Jan 28 08:21:37 host: servernameabc process: httpd[12345] ip1: 10.82.220.186 ip2: 0.1.0.1
session_id: 39714 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:37 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 393 response_time: 13 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #954 | Severity: High | Type: Data Exfiltration (Score: 19.9424)

```
Log Details:
syslog_ts: Jan 28 08:21:40 host: servernameabc process: httpd[12345] ip1: 10.181.196.130 ip2: 0.1.0.1
session_id: 33622 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:40 +0530 request: GET /favicon.ico
HTTP/1.1 status: 200 bytes: 3661 response_time: 33 referer: https://abc.example.com/index.html user_agent:
Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0
Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #958 | Severity: High | Type: Data Exfiltration (Score: 15.3106)

```
Log Details:
syslog_ts: Jan 28 08:21:44 host: servernameabc process: httpd[12345] ip1: 10.141.197.36 ip2: 0.1.0.1
session_id: 43214 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:44 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 1827 response_time: 8 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #961 | Severity: High | Type: Data Exfiltration (Score: 20.6812)

```
Log Details:
syslog_ts: Jan 28 08:21:46 host: servernameabc process: httpd[12345] ip1: 10.156.24.68 ip2: 0.1.0.1 session_id: 55845 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:46 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 6161 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #962 | Severity: High | Type: Data Exfiltration (Score: 21.6788)

```
Log Details:
syslog_ts: Jan 28 08:21:47 host: servernameabc process: httpd[12345] ip1: 10.174.8.48 ip2: 0.1.0.1 session_id: 16839 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:47 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 6865 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #966 | Severity: High | Type: Data Exfiltration (Score: 17.9451)

```
Log Details:
syslog_ts: Jan 28 08:21:49 host: servernameabc process: httpd[12345] ip1: 10.123.30.217 ip2: 0.1.0.1 session_id: 28857 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:49 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 2378 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #968 | Severity: High | Type: Data Exfiltration (Score: 23.3605)

```
Log Details:
syslog_ts: Jan 28 08:21:50 host: servernameabc process: httpd[12345] ip1: 10.53.216.211 ip2: 0.1.0.1 session_id: 56673 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:50 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 8200 response_time: 32 referer: https://abc.example.com/index.html user_agent:
```

```
Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #970 | Severity: High | Type: Data Exfiltration (Score: 26.3854)

```
Log Details:
syslog_ts: Jan 28 08:21:52 host: servernameabc process: httpd[12345] ip1: 10.72.178.48 ip2: 0.1.0.1 session_id: 54797 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:52 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 13575 response_time: 47 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #971 | Severity: High | Type: Data Exfiltration (Score: 23.3418)

```
Log Details:
syslog_ts: Jan 28 08:21:52 host: servernameabc process: httpd[12345] ip1: 10.50.130.3 ip2: 0.1.0.1 session_id: 87585 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:52 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 9460 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #972 | Severity: High | Type: Data Exfiltration (Score: 12.2819)

```
Log Details:
syslog_ts: Jan 28 08:21:53 host: servernameabc process: httpd[12345] ip1: 10.57.186.6 ip2: 0.1.0.1 session_id: 75904 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:53 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 724 response_time: 10 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #974 | Severity: High | Type: Data Exfiltration (Score: 25.1948)

Log Details:

syslog_ts: Jan 28 08:21:54 host: servernameabc process: httpd[12345] ip1: 10.114.16.23 ip2: 0.1.0.1 session_id: 67888 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:54 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 10819 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #975 | Severity: High | Type: Data Exfiltration (Score: 23.3062)

Log Details:

syslog_ts: Jan 28 08:21:54 host: servernameabc process: httpd[12345] ip1: 10.177.120.195 ip2: 0.1.0.1 session_id: 96672 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:54 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 6757 response_time: 50 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #976 | Severity: High | Type: Data Exfiltration (Score: 21.3343)

Log Details:

syslog_ts: Jan 28 08:21:55 host: servernameabc process: httpd[12345] ip1: 10.20.139.141 ip2: 0.1.0.1 session_id: 72381 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:55 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 7147 response_time: 12 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #977 | Severity: High | Type: Data Exfiltration (Score: 24.5809)

Log Details:

syslog_ts: Jan 28 08:21:57 host: servernameabc process: httpd[12345] ip1: 10.5.126.24 ip2: 0.1.0.1 session_id: 75547 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:57 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 9743 response_time: 41 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #978 | Severity: High | Type: Data Exfiltration (Score: 20.4651)

```
Log Details:
syslog_ts: Jan 28 08:21:58 host: servernameabc process: httpd[12345] ip1: 10.42.186.135 ip2: 0.1.0.1
session_id: 80373 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:58 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 5289 response_time: 17 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #979 | Severity: High | Type: Data Exfiltration (Score: 22.8524)

```
Log Details:
syslog_ts: Jan 28 08:21:58 host: servernameabc process: httpd[12345] ip1: 10.44.92.207 ip2: 0.1.0.1
session_id: 95370 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:58 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 6701 response_time: 40 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #982 | Severity: High | Type: Data Exfiltration (Score: 27.1388)

```
Log Details:
syslog_ts: Jan 28 08:22:01 host: servernameabc process: httpd[12345] ip1: 10.111.58.9 ip2: 0.1.0.1
session_id: 46120 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:01 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 18301 response_time: 32 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #984 | Severity: High | Type: Data Exfiltration (Score: 26.5422)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:22:04 host: servernameabc process: httpd[12345] ip1: 10.184.33.188 ip2: 0.1.0.1 session_id: 67753 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:04 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 16950 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #985 | Severity: High | Type: Data Exfiltration (Score: 26.0560)

```
Log Details:
syslog_ts: Jan 28 08:22:05 host: servernameabc process: httpd[12345] ip1: 10.26.106.39 ip2: 0.1.0.1 session_id: 13580 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:05 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 19969 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #986 | Severity: High | Type: Data Exfiltration (Score: 22.6790)

```
Log Details:
syslog_ts: Jan 28 08:22:06 host: servernameabc process: httpd[12345] ip1: 10.22.140.85 ip2: 0.1.0.1 session_id: 61953 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:06 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 8175 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #989 | Severity: High | Type: Data Exfiltration (Score: 13.2296)

```
Log Details:
syslog_ts: Jan 28 08:22:09 host: servernameabc process: httpd[12345] ip1: 10.49.187.40 ip2: 0.1.0.1 session_id: 69782 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:09 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 1106 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #992 | Severity: High | Type: Data Exfiltration (Score: 13.8783)

Log Details:

```
syslog_ts: Jan 28 08:22:12 host: servernameabc process: httpd[12345] ip1: 10.213.42.83 ip2: 0.1.0.1 session_id: 42734 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:12 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 769 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #993 | Severity: High | Type: Data Exfiltration (Score: 16.6852)

Log Details:

```
syslog_ts: Jan 28 08:22:12 host: servernameabc process: httpd[12345] ip1: 10.45.100.212 ip2: 0.1.0.1 session_id: 26549 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:12 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 200 bytes: 1923 response_time: 21 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #996 | Severity: High | Type: Data Exfiltration (Score: 26.4603)

Log Details:

```
syslog_ts: Jan 28 08:22:13 host: servernameabc process: httpd[12345] ip1: 10.200.238.69 ip2: 0.1.0.1 session_id: 90730 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:13 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 15922 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #998 | Severity: High | Type: Data Exfiltration (Score: 26.3259)

Log Details:

```
syslog_ts: Jan 28 08:22:15 host: servernameabc process: httpd[12345] ip1: 10.94.175.48 ip2: 0.1.0.1 session_id: 82974 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:15 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 17048 response_time: 24 referer: https://abc.example.com/index.html
```

user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high volume data transfer to a suspicious destination IP (0.1.0.1) with anomalous response times and sizes.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #3 | Severity: High | Type: Data Exfiltration (Score: 19.7006)

Log Details:

syslog_ts: Jan 28 08:10:04 host: servernameabc process: httpd[12345] ip1: 10.97.33.120 ip2: 0.1.0.1 session_id: 14285 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:04 +0530 request: GET /favicon.ico HTTP/1.1 status: 204 bytes: - response_time: 2764 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of high response times and anomalous file requests, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #8 | Severity: High | Type: Data Exfiltration (Score: 19.2154)

Log Details:

syslog_ts: Jan 28 08:10:06 host: servernameabc process: httpd[12345] ip1: 10.189.232.208 ip2: 0.1.0.1 session_id: 45431 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:06 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 204 bytes: - response_time: 2443 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of high response times and anomalous file requests, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #288 | Severity: High | Type: Data Exfiltration (Score: 18.9423)

Log Details:

syslog_ts: Jan 28 08:13:22 host: servernameabc process: httpd[12345] ip1: 10.165.149.161 ip2: 0.1.0.1 session_id: 43706 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:22 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 2277 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of high response times and anomalous file requests, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #348 | Severity: High | Type: Data Exfiltration (Score: 18.8739)

Log Details:

```
syslog_ts: Jan 28 08:14:10 host: servernameabc process: httpd[12345] ip1: 10.149.45.206 ip2: 0.1.0.1 session_id: 31559 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:10 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 2237 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high response times and anomalous file requests, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #477 | Severity: High | Type: Data Exfiltration (Score: 18.5337)

Log Details:

```
syslog_ts: Jan 28 08:15:37 host: servernameabc process: httpd[12345] ip1: 10.252.73.37 ip2: 0.1.0.1 session_id: 71508 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:37 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 2047 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high response times and anomalous file requests, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #557 | Severity: High | Type: Data Exfiltration (Score: 19.0446)

Log Details:

```
syslog_ts: Jan 28 08:16:35 host: servernameabc process: httpd[12345] ip1: 10.160.105.182 ip2: 0.1.0.1 session_id: 77303 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:35 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 2338 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high response times and anomalous file requests, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #645 | Severity: High | Type: Data Exfiltration (Score: 19.2567)

Log Details:

```
syslog_ts: Jan 28 08:17:47 host: servernameabc process: httpd[12345] ip1: 10.162.176.72 ip2: 0.1.0.1 session_id: 65318 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:47 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 2469 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a consistent pattern of high response times and anomalous file requests, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #868 | Severity: High | Type: Data Exfiltration (Score: 19.1624)

Log Details:

```
syslog_ts: Jan 28 08:20:37 host: servernameabc process: httpd[12345] ip1: 10.123.199.59 ip2: 0.1.0.1 session_id: 86050 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:37 +0530 request: GET /favicon.ico HTTP/1.1 status: 204 bytes: - response_time: 2410 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of high response times and anomalous file requests, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #887 | Severity: High | Type: Data Exfiltration (Score: 19.6992)

Log Details:

```
syslog_ts: Jan 28 08:20:52 host: servernameabc process: httpd[12345] ip1: 10.10.14.209 ip2: 0.1.0.1 session_id: 97202 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:52 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 2763 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of high response times and anomalous file requests, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #957 | Severity: High | Type: Data Exfiltration (Score: 19.0130)

Log Details:

```
syslog_ts: Jan 28 08:21:43 host: servernameabc process: httpd[12345] ip1: 10.130.224.231 ip2: 0.1.0.1 session_id: 20434 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:43 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 2319 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of high response times and anomalous file requests, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #14 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.6084)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:10:10 host: servernameabc process: httpd[12345] ip1: 10.223.164.203 ip2: 0.1.0.1 session_id: 19253 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:10 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 404 bytes: - response_time: 3465 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #94 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.7021)

```
Log Details:
syslog_ts: Jan 28 08:11:11 host: servernameabc process: httpd[12345] ip1: 10.243.203.197 ip2: 0.1.0.1 session_id: 60983 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:11 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 404 bytes: - response_time: 3545 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #122 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.9316)

```
Log Details:
syslog_ts: Jan 28 08:11:26 host: servernameabc process: httpd[12345] ip1: 10.133.201.236 ip2: 0.1.0.1 session_id: 39618 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:26 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 404 bytes: - response_time: 3749 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #176 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.9199)

```
Log Details:
syslog_ts: Jan 28 08:12:09 host: servernameabc process: httpd[12345] ip1: 10.221.174.154 ip2: 0.1.0.1 session_id: 90005 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:09 +0530 request: GET /favicon.ico HTTP/1.1 status: 404 bytes: - response_time: 4751 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #242 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.7432)

Log Details:

```
syslog_ts: Jan 28 08:12:54 host: servernameabc process: httpd[12345] ip1: 10.120.133.200 ip2: 0.1.0.1 session_id: 15160 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:54 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 404 bytes: - response_time: 3581 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #264 | Severity: High | Type: HTTP 404 Error Flood (Score: 10422.0127)

Log Details:

```
syslog_ts: Jan 28 08:13:06 host: servernameabc process: httpd[12345] ip1: 10.58.135.78 ip2: 0.1.0.1 session_id: 70795 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:06 +0530 request: GET /dashboard/stats HTTP/1.1 status: 404 bytes: - response_time: 4856 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #268 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.4727)

Log Details:

```
syslog_ts: Jan 28 08:13:10 host: servernameabc process: httpd[12345] ip1: 10.255.142.221 ip2: 0.1.0.1 session_id: 69936 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:10 +0530 request: GET /dashboard/stats HTTP/1.1 status: 404 bytes: - response_time: 4272 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #375 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.8594)

Log Details:

```
syslog_ts: Jan 28 08:14:32 host: servernameabc process: httpd[12345] ip1: 10.134.194.207 ip2: 0.1.0.1 session_id: 50798 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:32 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 404 bytes: - response_time: 3684 referer:
```

```
https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #452 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.6484)

```
Log Details:
syslog_ts: Jan 28 08:15:20  host: servernameabc  process: httpd[12345]  ip1: 10.96.94.244  ip2: 0.1.0.1  session_id: 37234  domain: abc.example.net  apache_ts: 28/Jan/2026:08:15:20 +0530  request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1  status: 404  bytes: -  response_time: 4455  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #573 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.8613)

```
Log Details:
syslog_ts: Jan 28 08:16:49  host: servernameabc  process: httpd[12345]  ip1: 10.241.24.52  ip2: 0.1.0.1  session_id: 77165  domain: abc.example.net  apache_ts: 28/Jan/2026:08:16:49 +0530  request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1  status: 404  bytes: -  response_time: 4686  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #580 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.4004)

```
Log Details:
syslog_ts: Jan 28 08:16:55  host: servernameabc  process: httpd[12345]  ip1: 10.119.12.50  ip2: 0.1.0.1  session_id: 63539  domain: abc.example.net  apache_ts: 28/Jan/2026:08:16:55 +0530  request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1  status: 404  bytes: -  response_time: 4199  referer: https://abc.example.com/index.html  user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #634 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.2637)

Log Details:

```
syslog_ts: Jan 28 08:17:38 host: servernameabc process: httpd[12345] ip1: 10.81.226.173 ip2: 0.1.0.1 session_id: 98383 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:38 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 404 bytes: - response_time: 3182 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #638 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.2783)

Log Details:

```
syslog_ts: Jan 28 08:17:41 host: servernameabc process: httpd[12345] ip1: 10.18.0.28 ip2: 0.1.0.1 session_id: 77662 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:41 +0530 request: GET /favicon.ico HTTP/1.1 status: 404 bytes: - response_time: 3194 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #689 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.1855)

Log Details:

```
syslog_ts: Jan 28 08:18:20 host: servernameabc process: httpd[12345] ip1: 10.185.104.220 ip2: 0.1.0.1 session_id: 65272 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:20 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 404 bytes: - response_time: 3987 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #724 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.7305)

Log Details:

```
syslog_ts: Jan 28 08:18:49 host: servernameabc process: httpd[12345] ip1: 10.158.203.254 ip2: 0.1.0.1 session_id: 41195 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:49 +0530 request: GET /dashboard/stats HTTP/1.1 status: 404 bytes: - response_time: 4543 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #776 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.8428)

Log Details:

```
syslog_ts: Jan 28 08:19:26 host: servernameabc process: httpd[12345] ip1: 10.204.159.158 ip2: 0.1.0.1 session_id: 67607 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:26 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 404 bytes: - response_time: 3669 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #833 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.3740)

Log Details:

```
syslog_ts: Jan 28 08:20:11 host: servernameabc process: httpd[12345] ip1: 10.162.20.11 ip2: 0.1.0.1 session_id: 48506 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:11 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 404 bytes: - response_time: 3270 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #916 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.1279)

Log Details:

```
syslog_ts: Jan 28 08:21:10 host: servernameabc process: httpd[12345] ip1: 10.184.166.223 ip2: 0.1.0.1 session_id: 42757 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:10 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 404 bytes: - response_time: 3932 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #918 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.6133)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:21:12 host: servernameabc process: httpd[12345] ip1: 10.126.197.226 ip2: 0.1.0.1 session_id: 34532 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:12 +0530 request: GET /dashboard/stats HTTP/1.1 status: 404 bytes: - response_time: 4418 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #955 | Severity: High | Type: HTTP 404 Error Flood (Score: 10419.7480)

Log Details:

```
syslog_ts: Jan 28 08:21:41 host: servernameabc process: httpd[12345] ip1: 10.2.214.167 ip2: 0.1.0.1 session_id: 23810 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:41 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 404 bytes: - response_time: 2797 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #964 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.8242)

Log Details:

```
syslog_ts: Jan 28 08:21:48 host: servernameabc process: httpd[12345] ip1: 10.167.196.68 ip2: 0.1.0.1 session_id: 98293 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:48 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 404 bytes: - response_time: 3653 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times, indicating a potential flood attack targeting specific resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #27 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.1602)

Log Details:

```
syslog_ts: Jan 28 08:10:19 host: servernameabc process: httpd[12345] ip1: 10.188.251.14 ip2: 0.1.0.1 session_id: 10989 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:19 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 404 bytes: - response_time: 2914 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of multiple HTTP POST requests resulting in 404 errors with high response times, indicating a potential flood attack.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #214 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.0244)

Log Details:

```
syslog_ts: Jan 28 08:12:35 host: servernameabc process: httpd[12345] ip1: 10.165.77.123 ip2: 0.1.0.1 session_id: 39225 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:35 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 404 bytes: - response_time: 2816 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of multiple HTTP POST requests resulting in 404 errors with high response times, indicating a potential flood attack.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #313 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.0986)

Log Details:

```
syslog_ts: Jan 28 08:13:42 host: servernameabc process: httpd[12345] ip1: 10.169.227.229 ip2: 0.1.0.1 session_id: 64219 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:42 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 404 bytes: - response_time: 2869 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a consistent pattern of multiple HTTP POST requests resulting in 404 errors with high response times, indicating a potential flood attack.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #628 | Severity: High | Type: HTTP 404 Error Flood (Score: 10419.9834)

Log Details:

```
syslog_ts: Jan 28 08:17:32 host: servernameabc process: httpd[12345] ip1: 10.57.122.4 ip2: 0.1.0.1 session_id: 47088 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:32 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 404 bytes: - response_time: 2787 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of multiple HTTP POST requests resulting in 404 errors with high response times, indicating a potential flood attack.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #657 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.3389)

Log Details:

```
syslog_ts: Jan 28 08:17:56 host: servernameabc process: httpd[12345] ip1: 10.69.161.242 ip2: 0.1.0.1 session_id: 72466 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:56 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 404 bytes: - response_time: 3047 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of multiple HTTP POST requests resulting in 404 errors with high response times, indicating a potential flood attack.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #758 | Severity: High | Type: HTTP 404 Error Flood (Score: 10420.2109)

Log Details:

syslog_ts: Jan 28 08:19:15 host: servernameabc process: httpd[12345] ip1: 10.229.106.20 ip2: 0.1.0.1 session_id: 47905 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:15 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 404 bytes: - response_time: 2951 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of multiple HTTP POST requests resulting in 404 errors with high response times, indicating a potential flood attack.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #796 | Severity: High | Type: HTTP 404 Error Flood (Score: 10419.8857)

Log Details:

syslog_ts: Jan 28 08:19:43 host: servernameabc process: httpd[12345] ip1: 10.117.14.225 ip2: 0.1.0.1 session_id: 18170 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:43 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 404 bytes: - response_time: 2719 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of multiple HTTP POST requests resulting in 404 errors with high response times, indicating a potential flood attack.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #33 | Severity: High | Type: DoS (Score: 22516.8086)

Log Details:

syslog_ts: Jan 28 08:10:24 host: servernameabc process: httpd[12345] ip1: 10.11.145.193 ip2: 0.1.0.1 session_id: 42810 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:24 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 500 bytes: - response_time: 3422 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a series of HTTP POST requests with high response times and status code 500, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #204 | Severity: High | Type: DoS (Score: 22516.9883)

Log Details:

```
syslog_ts: Jan 28 08:12:28 host: servernameabc process: httpd[12345] ip1: 10.99.165.124 ip2: 0.1.0.1 session_id: 81843 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:28 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 500 bytes: - response_time: 3576 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a series of HTTP POST requests with high response times and status code 500, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #218 | Severity: High | Type: DoS (Score: 22514.6543)

Log Details:

```
syslog_ts: Jan 28 08:12:39 host: servernameabc process: httpd[12345] ip1: 10.105.5.21 ip2: 0.1.0.1 session_id: 66798 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:39 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 500 bytes: - response_time: 1978 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a series of HTTP POST requests with high response times and status code 500, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #261 | Severity: High | Type: DoS (Score: 22516.6230)

Log Details:

```
syslog_ts: Jan 28 08:13:05 host: servernameabc process: httpd[12345] ip1: 10.25.38.189 ip2: 0.1.0.1 session_id: 69571 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:05 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 500 bytes: - response_time: 3270 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a series of HTTP POST requests with high response times and status code 500, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #594 | Severity: High | Type: DoS (Score: 22513.9180)

Log Details:

```
syslog_ts: Jan 28 08:17:06 host: servernameabc process: httpd[12345] ip1: 10.95.34.112 ip2: 0.1.0.1 session_id: 46712 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:06 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 500 bytes: - response_time: 1625 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a series of HTTP POST requests with high response times and status code 500, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #707 | Severity: High | Type: DoS (Score: 22513.8301)

```
Log Details:
syslog_ts: Jan 28 08:18:33 host: servernameabc process: httpd[12345] ip1: 10.247.134.125 ip2: 0.1.0.1 session_id: 21418 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:33 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 500 bytes: - response_time: 1587 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a series of HTTP POST requests with high response times and status code 500, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #44 | Severity: High | Type: Data Exfiltration (Score: 15.3746)

```
Log Details:
syslog_ts: Jan 28 08:10:32 host: servernameabc process: httpd[12345] ip1: 10.235.179.53 ip2: 0.1.0.1 session_id: 34867 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:32 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 849 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a series of HTTP GET requests with high response times and no data transferred, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #451 | Severity: High | Type: Data Exfiltration (Score: 15.7744)

```
Log Details:
syslog_ts: Jan 28 08:15:19 host: servernameabc process: httpd[12345] ip1: 10.153.107.158 ip2: 0.1.0.1 session_id: 43830 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:19 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 204 bytes: - response_time: 955 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a series of HTTP GET requests with high response times and no data transferred, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #489 | Severity: High | Type: Data Exfiltration (Score: 14.9298)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:15:48 host: servernameabc process: httpd[12345] ip1: 10.107.19.175 ip2: 0.1.0.1 session_id: 89514 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:48 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 743 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a series of HTTP GET requests with high response times and no data transferred, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #550 | Severity: High | Type: Data Exfiltration (Score: 15.3467)

Log Details:

```
syslog_ts: Jan 28 08:16:28 host: servernameabc process: httpd[12345] ip1: 10.199.254.191 ip2: 0.1.0.1 session_id: 94089 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:28 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 842 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a series of HTTP GET requests with high response times and no data transferred, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #618 | Severity: High | Type: Data Exfiltration (Score: 14.8806)

Log Details:

```
syslog_ts: Jan 28 08:17:24 host: servernameabc process: httpd[12345] ip1: 10.231.61.239 ip2: 0.1.0.1 session_id: 30698 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:24 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 732 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a series of HTTP GET requests with high response times and no data transferred, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #641 | Severity: High | Type: Data Exfiltration (Score: 16.4046)

Log Details:

```
syslog_ts: Jan 28 08:17:43 host: servernameabc process: httpd[12345] ip1: 10.17.80.115 ip2: 0.1.0.1 session_id: 28190 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:43 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 1145 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a series of HTTP GET requests with high response times and no data transferred, indicating potential data exfiltration attempts.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #675 | Severity: High | Type: Data Exfiltration (Score: 16.8719)

Log Details:

```
syslog_ts: Jan 28 08:18:08 host: servernameabc process: httpd[12345] ip1: 10.126.130.107 ip2: 0.1.0.1 session_id: 11791 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:08 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 204 bytes: - response_time: 1306 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a series of HTTP GET requests with high response times and no data transferred, indicating potential data exfiltration attempts.

Reason for Detection:

This log is part of an anomaly cluster 'Data Exfiltration'. Contributing features: Status, Size, Duration.

Anomaly #58 | Severity: High | Type: DoS (Score: 22966.3145)

Log Details:

```
syslog_ts: Jan 28 08:10:42 host: servernameabc process: httpd[12345] ip1: 10.238.151.32 ip2: 0.1.0.1 session_id: 34917 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:42 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 503 bytes: - response_time: 1808 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #130 | Severity: High | Type: DoS (Score: 22968.3594)

Log Details:

```
syslog_ts: Jan 28 08:11:33 host: servernameabc process: httpd[12345] ip1: 10.153.69.190 ip2: 0.1.0.1 session_id: 16525 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:33 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 503 bytes: - response_time: 3063 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #133 | Severity: High | Type: DoS (Score: 22968.5645)

Log Details:

```
syslog_ts: Jan 28 08:11:35 host: servernameabc process: httpd[12345] ip1: 10.168.36.123 ip2: 0.1.0.1 session_id: 44707 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:35 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 503 bytes: - response_time: 3223 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #154 | Severity: High | Type: DoS (Score: 22969.9980)

Log Details:

syslog_ts: Jan 28 08:11:50 host: servernameabc process: httpd[12345] ip1: 10.222.112.120 ip2: 0.1.0.1 session_id: 72623 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:50 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 503 bytes: - response_time: 4562 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #164 | Severity: High | Type: DoS (Score: 22969.3086)

Log Details:

syslog_ts: Jan 28 08:11:59 host: servernameabc process: httpd[12345] ip1: 10.221.132.84 ip2: 0.1.0.1 session_id: 61461 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:59 +0530 request: GET /favicon.ico HTTP/1.1 status: 503 bytes: - response_time: 3866 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #217 | Severity: High | Type: DoS (Score: 22966.5312)

Log Details:

syslog_ts: Jan 28 08:12:38 host: servernameabc process: httpd[12345] ip1: 10.109.243.210 ip2: 0.1.0.1 session_id: 37980 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:38 +0530 request: GET /favicon.ico HTTP/1.1 status: 503 bytes: - response_time: 1915 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #359 | Severity: High | Type: DoS (Score: 22967.1973)

Log Details:

syslog_ts: Jan 28 08:14:20 host: servernameabc process: httpd[12345] ip1: 10.61.50.124 ip2: 0.1.0.1 session_id: 90168 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:20 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 503 bytes: - response_time: 2280 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #386 | Severity: High | Type: DoS (Score: 22968.2891)

Log Details:

syslog_ts: Jan 28 08:14:38 host: servernameabc process: httpd[12345] ip1: 10.78.92.126 ip2: 0.1.0.1 session_id: 70318 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:38 +0530 request: GET /favicon.ico HTTP/1.1 status: 503 bytes: - response_time: 3009 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #392 | Severity: High | Type: DoS (Score: 22970.1113)

Log Details:

syslog_ts: Jan 28 08:14:43 host: servernameabc process: httpd[12345] ip1: 10.131.15.127 ip2: 0.1.0.1 session_id: 14627 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:43 +0530 request: GET /favicon.ico HTTP/1.1 status: 503 bytes: - response_time: 4685 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #433 | Severity: High | Type: DoS (Score: 22969.6094)

Log Details:

syslog_ts: Jan 28 08:15:08 host: servernameabc process: httpd[12345] ip1: 10.142.96.110 ip2: 0.1.0.1 session_id: 61497 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:08 +0530 request: GET /dashboard/stats HTTP/1.1 status: 503 bytes: - response_time: 4158 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

Anomaly Detection Report

The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #667 | Severity: High | Type: DoS (Score: 22970.2637)

Log Details:

```
syslog_ts: Jan 28 08:18:03 host: servernameabc process: httpd[12345] ip1: 10.56.118.157 ip2: 0.1.0.1 session_id: 67470 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:03 +0530 request: GET /dashboard/stats HTTP/1.1 status: 503 bytes: - response_time: 4858 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #877 | Severity: High | Type: DoS (Score: 22968.6406)

Log Details:

```
syslog_ts: Jan 28 08:20:44 host: servernameabc process: httpd[12345] ip1: 10.201.12.223 ip2: 0.1.0.1 session_id: 37283 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:44 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 503 bytes: - response_time: 3284 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high number of HTTP requests with status code 503 and unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #66 | Severity: High | Type: DDoS (Score: 20.8236)

Log Details:

```
syslog_ts: Jan 28 08:10:48 host: servernameabc process: httpd[12345] ip1: 10.138.99.2 ip2: 0.1.0.1 session_id: 21279 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:48 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 204 bytes: - response_time: 3652 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #277 | Severity: High | Type: DDoS (Score: 21.4786)

Log Details:

```
syslog_ts: Jan 28 08:13:16 host: servernameabc process: httpd[12345] ip1: 10.191.228.102 ip2: 0.1.0.1
```

Anomaly Detection Report

session_id: 45251 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:16 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 4278 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #285 | Severity: High | Type: DDoS (Score: 21.7869)

Log Details:

syslog_ts: Jan 28 08:13:20 host: servernameabc process: httpd[12345] ip1: 10.136.136.134 ip2: 0.1.0.1 session_id: 82224 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:20 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 4604 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #321 | Severity: High | Type: DDoS (Score: 21.7446)

Log Details:

syslog_ts: Jan 28 08:13:49 host: servernameabc process: httpd[12345] ip1: 10.73.214.61 ip2: 0.1.0.1 session_id: 86773 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:49 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 4558 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #353 | Severity: High | Type: DDoS (Score: 21.1025)

Log Details:

syslog_ts: Jan 28 08:14:15 host: servernameabc process: httpd[12345] ip1: 10.4.119.13 ip2: 0.1.0.1 session_id: 32037 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:15 +0530 request: GET /favicon.ico HTTP/1.1 status: 204 bytes: - response_time: 3908 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #411 | Severity: High | Type: DDoS (Score: 20.8705)

Anomaly Detection Report

Log Details:

syslog_ts: Jan 28 08:14:55 host: servernameabc process: httpd[12345] ip1: 10.197.82.220 ip2: 0.1.0.1 session_id: 94973 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:55 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 204 bytes: - response_time: 3694 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #414 | Severity: High | Type: DDoS (Score: 19.8403)

Log Details:

syslog_ts: Jan 28 08:14:56 host: servernameabc process: httpd[12345] ip1: 10.31.129.8 ip2: 0.1.0.1 session_id: 83272 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:56 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 2863 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #439 | Severity: High | Type: DDoS (Score: 20.4326)

Log Details:

syslog_ts: Jan 28 08:15:13 host: servernameabc process: httpd[12345] ip1: 10.64.104.165 ip2: 0.1.0.1 session_id: 20751 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:13 +0530 request: GET /favicon.ico HTTP/1.1 status: 204 bytes: - response_time: 3318 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #493 | Severity: High | Type: DDoS (Score: 20.9803)

Log Details:

syslog_ts: Jan 28 08:15:50 host: servernameabc process: httpd[12345] ip1: 10.62.248.152 ip2: 0.1.0.1 session_id: 63445 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:50 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 3794 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #545 | Severity: High | Type: DDoS (Score: 20.9004)

Log Details:

syslog_ts: Jan 28 08:16:24 host: servernameabc process: httpd[12345] ip1: 10.89.214.79 ip2: 0.1.0.1 session_id: 64044 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:24 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 3721 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #646 | Severity: High | Type: DDoS (Score: 20.4968)

Log Details:

syslog_ts: Jan 28 08:17:47 host: servernameabc process: httpd[12345] ip1: 10.122.111.144 ip2: 0.1.0.1 session_id: 60353 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:47 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 3371 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #710 | Severity: High | Type: DDoS (Score: 21.2009)

Log Details:

syslog_ts: Jan 28 08:18:36 host: servernameabc process: httpd[12345] ip1: 10.184.77.109 ip2: 0.1.0.1 session_id: 29599 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:36 +0530 request: GET /favicon.ico HTTP/1.1 status: 204 bytes: - response_time: 4002 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #781 | Severity: High | Type: DDoS (Score: 20.7145)

Log Details:

syslog_ts: Jan 28 08:19:30 host: servernameabc process: httpd[12345] ip1: 10.218.159.96 ip2: 0.1.0.1 session_id: 94127 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:30 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 3556 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #816 | Severity: High | Type: DDoS (Score: 21.8343)

Log Details:

```
syslog_ts: Jan 28 08:19:57 host: servernameabc process: httpd[12345] ip1: 10.92.195.105 ip2: 0.1.0.1 session_id: 95107 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:57 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 4656 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #870 | Severity: High | Type: DDoS (Score: 21.8179)

Log Details:

```
syslog_ts: Jan 28 08:20:39 host: servernameabc process: httpd[12345] ip1: 10.86.136.52 ip2: 0.1.0.1 session_id: 99004 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:39 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 204 bytes: - response_time: 4638 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #905 | Severity: High | Type: DDoS (Score: 21.6437)

Log Details:

```
syslog_ts: Jan 28 08:21:02 host: servernameabc process: httpd[12345] ip1: 10.86.136.78 ip2: 0.1.0.1 session_id: 95078 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:02 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 4450 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly #981 | Severity: High | Type: DDoS (Score: 21.9719)

Log Details:

```
syslog_ts: Jan 28 08:22:00 host: servernameabc process: httpd[12345] ip1: 10.27.251.198 ip2: 0.1.0.1 session_id: 76740 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:00 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 4810 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high number of requests with similar status codes and response times, indicating a potential DDoS attack.

Reason for Detection:

This log is part of an anomaly cluster 'DDoS'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #84 | Severity: High | Type: DoS (Score: 20.1166)

Log Details:

```
syslog_ts: Jan 28 08:11:03 host: servernameabc process: httpd[12345] ip1: 10.187.150.89 ip2: 0.1.0.1 session_id: 36766 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:03 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 204 bytes: - response_time: 2882 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #86 | Severity: High | Type: DoS (Score: 21.4942)

Log Details:

```
syslog_ts: Jan 28 08:11:04 host: servernameabc process: httpd[12345] ip1: 10.76.138.126 ip2: 0.1.0.1 session_id: 72198 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:04 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 204 bytes: - response_time: 4044 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #107 | Severity: High | Type: DoS (Score: 22.1794)

Log Details:

```
syslog_ts: Jan 28 08:11:20 host: servernameabc process: httpd[12345] ip1: 10.225.144.131 ip2: 0.1.0.1 session_id: 35278 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:20 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 204 bytes: - response_time: 4762 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #206 | Severity: High | Type: DoS (Score: 18.9696)

Log Details:

```
syslog_ts: Jan 28 08:12:30 host: servernameabc process: httpd[12345] ip1: 10.144.252.138 ip2: 0.1.0.1 session_id: 15399 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:30 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 204 bytes: - response_time: 2149 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #278 | Severity: High | Type: DoS (Score: 17.6281)

Log Details:

```
syslog_ts: Jan 28 08:13:16 host: servernameabc process: httpd[12345] ip1: 10.130.106.30 ip2: 0.1.0.1 session_id: 88624 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:16 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 204 bytes: - response_time: 1502 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #327 | Severity: High | Type: DoS (Score: 20.6801)

Log Details:

```
syslog_ts: Jan 28 08:13:55 host: servernameabc process: httpd[12345] ip1: 10.110.158.112 ip2: 0.1.0.1 session_id: 21576 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:55 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 204 bytes: - response_time: 3316 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #355 | Severity: High | Type: DoS (Score: 19.5083)

Log Details:

```
syslog_ts: Jan 28 08:14:17 host: servernameabc process: httpd[12345] ip1: 10.255.101.215 ip2: 0.1.0.1 session_id: 64913 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:17 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 204 bytes: - response_time: 2470 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #422 | Severity: High | Type: DoS (Score: 22.2272)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:15:02 host: servernameabc process: httpd[12345] ip1: 10.6.207.103 ip2: 0.1.0.1 session_id: 39308 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:02 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 204 bytes: - response_time: 4816 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #445 | Severity: High | Type: DoS (Score: 21.0068)

Log Details:

```
syslog_ts: Jan 28 08:15:17 host: servernameabc process: httpd[12345] ip1: 10.60.145.71 ip2: 0.1.0.1 session_id: 51051 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:17 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 204 bytes: - response_time: 3593 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #458 | Severity: High | Type: DoS (Score: 17.4745)

Log Details:

```
syslog_ts: Jan 28 08:15:23 host: servernameabc process: httpd[12345] ip1: 10.225.208.242 ip2: 0.1.0.1 session_id: 22791 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:23 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 204 bytes: - response_time: 1440 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #491 | Severity: High | Type: DoS (Score: 20.9241)

Log Details:

```
syslog_ts: Jan 28 08:15:50 host: servernameabc process: httpd[12345] ip1: 10.35.196.159 ip2: 0.1.0.1 session_id: 94170 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:50 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 204 bytes: - response_time: 3521 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #496 | Severity: High | Type: DoS (Score: 19.7589)

Log Details:

```
syslog_ts: Jan 28 08:15:52 host: servernameabc process: httpd[12345] ip1: 10.143.29.194 ip2: 0.1.0.1 session_id: 39955 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:52 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 204 bytes: - response_time: 2633 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #510 | Severity: High | Type: DoS (Score: 18.1042)

Log Details:

```
syslog_ts: Jan 28 08:16:00 host: servernameabc process: httpd[12345] ip1: 10.226.240.87 ip2: 0.1.0.1 session_id: 97445 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:00 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 204 bytes: - response_time: 1709 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #525 | Severity: High | Type: DoS (Score: 21.4374)

Log Details:

```
syslog_ts: Jan 28 08:16:13 host: servernameabc process: httpd[12345] ip1: 10.13.112.152 ip2: 0.1.0.1 session_id: 94447 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:13 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 204 bytes: - response_time: 3989 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #578 | Severity: High | Type: DoS (Score: 21.7830)

Log Details:

```
syslog_ts: Jan 28 08:16:53 host: servernameabc process: httpd[12345] ip1: 10.104.223.118 ip2: 0.1.0.1 session_id: 41487 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:53 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 204 bytes: - response_time: 4334 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #692 | Severity: High | Type: DoS (Score: 19.8594)

Log Details:

syslog_ts: Jan 28 08:18:23 host: servernameabc process: httpd[12345] ip1: 10.128.89.35 ip2: 0.1.0.1 session_id: 56578 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:23 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 204 bytes: - response_time: 2701 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #748 | Severity: High | Type: DoS (Score: 21.7655)

Log Details:

syslog_ts: Jan 28 08:19:07 host: servernameabc process: httpd[12345] ip1: 10.213.159.15 ip2: 0.1.0.1 session_id: 76284 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:07 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 204 bytes: - response_time: 4316 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #831 | Severity: High | Type: DoS (Score: 20.1879)

Log Details:

syslog_ts: Jan 28 08:20:09 host: servernameabc process: httpd[12345] ip1: 10.178.171.46 ip2: 0.1.0.1 session_id: 36234 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:09 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 204 bytes: - response_time: 2934 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #995 | Severity: High | Type: DoS (Score: 18.3352)

```
Log Details:
syslog_ts: Jan 28 08:22:13 host: servernameabc process: httpd[12345] ip1: 10.122.0.115 ip2: 0.1.0.1
session_id: 60460 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:13 +0530 request: POST
/leaverest/rest/lwpBatch HTTP/1.1 status: 204 bytes: - response_time: 1818 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high number of POST requests with unusually high response times, indicating a potential Denial of Service attack.

Reason for Detection:

This log is part of an anomaly cluster 'DoS'. Contributing features: Status, Size, Duration.

Anomaly #95 | Severity: High | Type: HTTP 404 Error Flood (Score: 10422.0537)

```
Log Details:
syslog_ts: Jan 28 08:11:12 host: servernameabc process: httpd[12345] ip1: 10.158.192.60 ip2: 0.1.0.1
session_id: 68574 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:12 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 404 bytes: - response_time: 4622 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times and no bytes transferred, indicating a potential flood attack targeting the authentication endpoint.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #287 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.9961)

```
Log Details:
syslog_ts: Jan 28 08:13:22 host: servernameabc process: httpd[12345] ip1: 10.235.157.73 ip2: 0.1.0.1
session_id: 97229 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:22 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 404 bytes: - response_time: 4560 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times and no bytes transferred, indicating a potential flood attack targeting the authentication endpoint.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #301 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.9961)

```
Log Details:
syslog_ts: Jan 28 08:13:33 host: servernameabc process: httpd[12345] ip1: 10.9.168.44 ip2: 0.1.0.1
session_id: 21866 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:33 +0530 request: POST
/api/v1/auth/login HTTP/1.1 status: 404 bytes: - response_time: 4560 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a high rate of HTTP 404 errors with consistent response times and no bytes transferred, indicating a potential flood attack targeting the authentication endpoint.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #425 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.2588)

Log Details:

```
syslog_ts: Jan 28 08:15:03 host: servernameabc process: httpd[12345] ip1: 10.31.60.163 ip2: 0.1.0.1 session_id: 78421 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:03 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 404 bytes: - response_time: 3820 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times and no bytes transferred, indicating a potential flood attack targeting the authentication endpoint.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #473 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.1084)

Log Details:

```
syslog_ts: Jan 28 08:15:33 host: servernameabc process: httpd[12345] ip1: 10.78.234.254 ip2: 0.1.0.1 session_id: 27167 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:33 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 404 bytes: - response_time: 3683 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times and no bytes transferred, indicating a potential flood attack targeting the authentication endpoint.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #636 | Severity: High | Type: HTTP 404 Error Flood (Score: 10422.0215)

Log Details:

```
syslog_ts: Jan 28 08:17:40 host: servernameabc process: httpd[12345] ip1: 10.254.30.173 ip2: 0.1.0.1 session_id: 85660 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:40 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 404 bytes: - response_time: 4587 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times and no bytes transferred, indicating a potential flood attack targeting the authentication endpoint.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #699 | Severity: High | Type: HTTP 404 Error Flood (Score: 10421.7578)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:18:27 host: servernameabc process: httpd[12345] ip1: 10.126.21.41 ip2: 0.1.0.1 session_id: 21149 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:27 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 404 bytes: - response_time: 4308 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with consistent response times and no bytes transferred, indicating a potential flood attack targeting the authentication endpoint.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #97 | Severity: High | Type: HTTP 500 Internal Server Error Flood (Score: 22517.0410)

Log Details:

```
syslog_ts: Jan 28 08:11:12 host: servernameabc process: httpd[12345] ip1: 10.208.250.59 ip2: 0.1.0.1 session_id: 70093 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:12 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 500 bytes: - response_time: 3850 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 500 errors with abnormal response times, indicating a potential flood attack targeting the server's resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #99 | Severity: High | Type: HTTP 500 Internal Server Error Flood (Score: 22517.6250)

Log Details:

```
syslog_ts: Jan 28 08:11:14 host: servernameabc process: httpd[12345] ip1: 10.161.227.99 ip2: 0.1.0.1 session_id: 47422 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:14 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 500 bytes: - response_time: 4430 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high rate of HTTP 500 errors with abnormal response times, indicating a potential flood attack targeting the server's resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #137 | Severity: High | Type: HTTP 500 Internal Server Error Flood (Score: 22516.8848)

Log Details:

```
syslog_ts: Jan 28 08:11:37 host: servernameabc process: httpd[12345] ip1: 10.166.128.35 ip2: 0.1.0.1 session_id: 34827 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:37 +0530 request: GET /dashboard/stats HTTP/1.1 status: 500 bytes: - response_time: 3706 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 500 errors with abnormal response times, indicating a potential flood attack targeting the server's resources.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #368 | Severity: High | Type: HTTP 500 Internal Server Error Flood (Score: 22516.8945)

Log Details:

```
syslog_ts: Jan 28 08:14:28 host: servernameabc process: httpd[12345] ip1: 10.19.208.57 ip2: 0.1.0.1 session_id: 12692 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:28 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 500 bytes: - response_time: 3716 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 500 errors with abnormal response times, indicating a potential flood attack targeting the server's resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #397 | Severity: High | Type: HTTP 500 Internal Server Error Flood (Score: 22517.3457)

Log Details:

```
syslog_ts: Jan 28 08:14:47 host: servernameabc process: httpd[12345] ip1: 10.195.55.189 ip2: 0.1.0.1 session_id: 93702 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:47 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 500 bytes: - response_time: 4144 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 500 errors with abnormal response times, indicating a potential flood attack targeting the server's resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #442 | Severity: High | Type: HTTP 500 Internal Server Error Flood (Score: 22516.9238)

Log Details:

```
syslog_ts: Jan 28 08:15:14 host: servernameabc process: httpd[12345] ip1: 10.136.1.233 ip2: 0.1.0.1 session_id: 46141 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:14 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 500 bytes: - response_time: 3742 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high rate of HTTP 500 errors with abnormal response times, indicating a potential flood attack targeting the server's resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #565 | Severity: High | Type: HTTP 500 Internal Server Error Flood (Score: 22516.9219)

Log Details:

```
syslog_ts: Jan 28 08:16:42 host: servernameabc process: httpd[12345] ip1: 10.47.139.68 ip2: 0.1.0.1 session_id: 96931 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:42 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 500 bytes: - response_time: 3741 referer:
```

Anomaly Detection Report

https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a high rate of HTTP 500 errors with abnormal response times, indicating a potential flood attack targeting the server's resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #697 | Severity: High | Type: HTTP 500 Internal Server Error Flood (Score: 22517.8086)

Log Details:

syslog_ts: Jan 28 08:18:26 host: servernameabc process: httpd[12345] ip1: 10.244.194.120 ip2: 0.1.0.1 session_id: 32257 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:26 +0530 request: GET /dashboard/stats HTTP/1.1 status: 500 bytes: - response_time: 4627 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a high rate of HTTP 500 errors with abnormal response times, indicating a potential flood attack targeting the server's resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #956 | Severity: High | Type: HTTP 500 Internal Server Error Flood (Score: 22517.0117)

Log Details:

syslog_ts: Jan 28 08:21:42 host: servernameabc process: httpd[12345] ip1: 10.17.245.27 ip2: 0.1.0.1 session_id: 29386 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:42 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 500 bytes: - response_time: 3823 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a high rate of HTTP 500 errors with abnormal response times, indicating a potential flood attack targeting the server's resources.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #116 | Severity: High | Type: HTTP 404 Error Flood (Score: 10417.6699)

Log Details:

syslog_ts: Jan 28 08:11:23 host: servernameabc process: httpd[12345] ip1: 10.115.251.129 ip2: 0.1.0.1 session_id: 90484 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:23 +0530 request: GET /dashboard/stats HTTP/1.1 status: 404 bytes: - response_time: 1626 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #385 | Severity: High | Type: HTTP 404 Error Flood (Score: 10419.1055)

Log Details:

```
syslog_ts: Jan 28 08:14:37 host: servernameabc process: httpd[12345] ip1: 10.46.40.163 ip2: 0.1.0.1 session_id: 56302 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:37 +0530 request: GET /favicon.ico HTTP/1.1 status: 404 bytes: - response_time: 2375 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #483 | Severity: High | Type: HTTP 404 Error Flood (Score: 10416.7549)

Log Details:

```
syslog_ts: Jan 28 08:15:43 host: servernameabc process: httpd[12345] ip1: 10.249.139.55 ip2: 0.1.0.1 session_id: 64222 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:43 +0530 request: GET /favicon.ico HTTP/1.1 status: 404 bytes: - response_time: 1264 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #511 | Severity: High | Type: HTTP 404 Error Flood (Score: 10418.3242)

Log Details:

```
syslog_ts: Jan 28 08:16:00 host: servernameabc process: httpd[12345] ip1: 10.83.21.41 ip2: 0.1.0.1 session_id: 34171 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:00 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 404 bytes: - response_time: 1937 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #548 | Severity: High | Type: HTTP 404 Error Flood (Score: 10418.0078)

Log Details:

```
syslog_ts: Jan 28 08:16:27 host: servernameabc process: httpd[12345] ip1: 10.239.156.105 ip2: 0.1.0.1 session_id: 83856 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:27 +0530 request: GET /favicon.ico HTTP/1.1 status: 404 bytes: - response_time: 1781 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #559 | Severity: High | Type: HTTP 404 Error Flood (Score: 10418.2109)

Log Details:

```
syslog_ts: Jan 28 08:16:37 host: servernameabc process: httpd[12345] ip1: 10.80.0.205 ip2: 0.1.0.1 session_id: 60009 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:37 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 404 bytes: - response_time: 1880 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #572 | Severity: High | Type: HTTP 404 Error Flood (Score: 10418.0498)

Log Details:

```
syslog_ts: Jan 28 08:16:48 host: servernameabc process: httpd[12345] ip1: 10.160.88.79 ip2: 0.1.0.1 session_id: 74501 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:48 +0530 request: GET /favicon.ico HTTP/1.1 status: 404 bytes: - response_time: 1801 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #603 | Severity: High | Type: HTTP 404 Error Flood (Score: 10417.5615)

Log Details:

```
syslog_ts: Jan 28 08:17:13 host: servernameabc process: httpd[12345] ip1: 10.97.131.107 ip2: 0.1.0.1 session_id: 29737 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:13 +0530 request: GET /dashboard/stats HTTP/1.1 status: 404 bytes: - response_time: 1579 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #608 | Severity: High | Type: HTTP 404 Error Flood (Score: 10417.9229)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:17:18 host: servernameabc process: httpd[12345] ip1: 10.77.230.116 ip2: 0.1.0.1 session_id: 34241 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:18 +0530 request: GET /dashboard/stats HTTP/1.1 status: 404 bytes: - response_time: 1741 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #609 | Severity: High | Type: HTTP 404 Error Flood (Score: 10418.6279)

```
Log Details:
syslog_ts: Jan 28 08:17:18 host: servernameabc process: httpd[12345] ip1: 10.120.169.107 ip2: 0.1.0.1 session_id: 92184 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:18 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 404 bytes: - response_time: 2098 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #660 | Severity: High | Type: HTTP 404 Error Flood (Score: 10417.7637)

```
Log Details:
syslog_ts: Jan 28 08:17:58 host: servernameabc process: httpd[12345] ip1: 10.115.25.28 ip2: 0.1.0.1 session_id: 54145 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:58 +0530 request: GET /favicon.ico HTTP/1.1 status: 404 bytes: - response_time: 1668 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #726 | Severity: High | Type: HTTP 404 Error Flood (Score: 10417.2246)

```
Log Details:
syslog_ts: Jan 28 08:18:50 host: servernameabc process: httpd[12345] ip1: 10.93.114.63 ip2: 0.1.0.1 session_id: 35972 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:50 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 404 bytes: - response_time: 1440 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Anomaly Detection Report

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #965 | Severity: High | Type: HTTP 404 Error Flood (Score: 10417.6221)

Log Details:

```
syslog_ts: Jan 28 08:21:49 host: servernameabc process: httpd[12345] ip1: 10.122.210.23 ip2: 0.1.0.1 session_id: 45494 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:49 +0530 request: GET /dashboard/stats HTTP/1.1 status: 404 bytes: - response_time: 1605 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #980 | Severity: High | Type: HTTP 404 Error Flood (Score: 10417.7393)

Log Details:

```
syslog_ts: Jan 28 08:21:59 host: servernameabc process: httpd[12345] ip1: 10.65.165.76 ip2: 0.1.0.1 session_id: 31622 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:59 +0530 request: GET /dashboard/stats HTTP/1.1 status: 404 bytes: - response_time: 1657 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a high rate of HTTP 404 errors with anomalous response times, indicating a potential flood attack targeting specific URLs.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 404 Error Flood'. Contributing features: Status, Size, Duration.

Anomaly #238 | Severity: High | Type: HTTP 500 Internal Server Error (Score: 22513.8652)

Log Details:

```
syslog_ts: Jan 28 08:12:52 host: servernameabc process: httpd[12345] ip1: 10.51.43.242 ip2: 0.1.0.1 session_id: 64237 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:52 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 500 bytes: - response_time: 1714 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of HTTP 500 errors across multiple logs, indicating a potential server-side issue or misconfiguration.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error'. Contributing features: Status, Size, Duration.

Anomaly #248 | Severity: High | Type: HTTP 500 Internal Server Error (Score: 22513.9824)

Log Details:

```
syslog_ts: Jan 28 08:12:57 host: servernameabc process: httpd[12345] ip1: 10.233.159.247 ip2: 0.1.0.1 session_id: 33676 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:57 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 500 bytes: - response_time: 1769 referer:
```

https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of HTTP 500 errors across multiple logs, indicating a potential server-side issue or misconfiguration.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error'. Contributing features: Status, Size, Duration.

Anomaly #328 | Severity: High | Type: HTTP 500 Internal Server Error (Score: 22514.2988)

Log Details:

syslog_ts: Jan 28 08:13:55 host: servernameabc process: httpd[12345] ip1: 10.87.154.69 ip2: 0.1.0.1 session_id: 64444 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:55 +0530 request: GET /dashboard/stats HTTP/1.1 status: 500 bytes: - response_time: 1924 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The cluster shows a consistent pattern of HTTP 500 errors across multiple logs, indicating a potential server-side issue or misconfiguration.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error'. Contributing features: Status, Size, Duration.

Anomaly #532 | Severity: High | Type: HTTP 500 Internal Server Error (Score: 22514.5781)

Log Details:

syslog_ts: Jan 28 08:16:17 host: servernameabc process: httpd[12345] ip1: 10.75.11.170 ip2: 0.1.0.1 session_id: 65457 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:17 +0530 request: GET /dashboard/stats HTTP/1.1 status: 500 bytes: - response_time: 2071 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The cluster shows a consistent pattern of HTTP 500 errors across multiple logs, indicating a potential server-side issue or misconfiguration.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error'. Contributing features: Status, Size, Duration.

Anomaly #704 | Severity: High | Type: HTTP 500 Internal Server Error (Score: 22514.8574)

Log Details:

syslog_ts: Jan 28 08:18:32 host: servernameabc process: httpd[12345] ip1: 10.112.204.31 ip2: 0.1.0.1 session_id: 20724 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:32 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 500 bytes: - response_time: 2228 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The cluster shows a consistent pattern of HTTP 500 errors across multiple logs, indicating a potential server-side issue or misconfiguration.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error'. Contributing features: Status, Size, Duration.

Anomaly Detection Report

Anomaly #766 | Severity: High | Type: HTTP 500 Internal Server Error (Score: 22514.7793)

Log Details:

```
syslog_ts: Jan 28 08:19:20 host: servernameabc process: httpd[12345] ip1: 10.45.140.143 ip2: 0.1.0.1 session_id: 24716 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:20 +0530 request: GET /dashboard/stats HTTP/1.1 status: 500 bytes: - response_time: 2183 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The cluster shows a consistent pattern of HTTP 500 errors across multiple logs, indicating a potential server-side issue or misconfiguration.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error'. Contributing features: Status, Size, Duration.

Anomaly #783 | Severity: High | Type: HTTP 500 Internal Server Error (Score: 22515.7070)

Log Details:

```
syslog_ts: Jan 28 08:19:31 host: servernameabc process: httpd[12345] ip1: 10.22.178.156 ip2: 0.1.0.1 session_id: 70010 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:31 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 500 bytes: - response_time: 2768 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The cluster shows a consistent pattern of HTTP 500 errors across multiple logs, indicating a potential server-side issue or misconfiguration.

Reason for Detection:

This log is part of an anomaly cluster 'HTTP 500 Internal Server Error'. Contributing features: Status, Size, Duration.

Anomaly #21 | Severity: Low | Type: Isolated Anomaly (Score: 14.0107)

Log Details:

```
syslog_ts: Jan 28 08:10:16 host: servernameabc process: httpd[12345] ip1: 10.117.55.88 ip2: 0.1.0.1 session_id: 69500 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:16 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 559 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #26 | Severity: Low | Type: Isolated Anomaly (Score: 10419.1475)

Log Details:

```
syslog_ts: Jan 28 08:10:19 host: servernameabc process: httpd[12345] ip1: 10.128.191.12 ip2: 0.1.0.1 session_id: 72021 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:19 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 404 bytes: - response_time: 2401 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

N/A

Anomaly Detection Report

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #96 | Severity: Low | Type: Isolated Anomaly (Score: 22962.4824)

Log Details:

syslog_ts: Jan 28 08:11:12 host: servernameabc process: httpd[12345] ip1: 10.14.184.24 ip2: 0.1.0.1 session_id: 63367 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:12 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 503 bytes: - response_time: 554 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #100 | Severity: Low | Type: Isolated Anomaly (Score: 10416.1201)

Log Details:

syslog_ts: Jan 28 08:11:14 host: servernameabc process: httpd[12345] ip1: 10.129.38.198 ip2: 0.1.0.1 session_id: 44349 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:14 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 404 bytes: - response_time: 982 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #120 | Severity: Low | Type: Isolated Anomaly (Score: 10416.6465)

Log Details:

syslog_ts: Jan 28 08:11:26 host: servernameabc process: httpd[12345] ip1: 10.178.67.188 ip2: 0.1.0.1 session_id: 14783 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:26 +0530 request: GET /dashboard/stats HTTP/1.1 status: 404 bytes: - response_time: 1226 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #134 | Severity: Low | Type: Isolated Anomaly (Score: 16.5406)

Log Details:

syslog_ts: Jan 28 08:11:35 host: servernameabc process: httpd[12345] ip1: 10.75.208.217 ip2: 0.1.0.1 session_id: 12518 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:35 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 1190 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

Anomaly Detection Report

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #144 | Severity: Low | Type: Isolated Anomaly (Score: 22511.9512)

Log Details:

syslog_ts: Jan 28 08:11:41 host: servernameabc process: httpd[12345] ip1: 10.172.81.245 ip2: 0.1.0.1 session_id: 16207 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:41 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 500 bytes: - response_time: 935 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #156 | Severity: Low | Type: Isolated Anomaly (Score: 10417.1875)

Log Details:

syslog_ts: Jan 28 08:11:52 host: servernameabc process: httpd[12345] ip1: 10.134.39.199 ip2: 0.1.0.1 session_id: 33858 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:52 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 404 bytes: - response_time: 1330 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #172 | Severity: Low | Type: Isolated Anomaly (Score: 18.3103)

Log Details:

syslog_ts: Jan 28 08:12:06 host: servernameabc process: httpd[12345] ip1: 10.180.42.234 ip2: 0.1.0.1 session_id: 55628 domain: abc.example.net apache_ts: 28/Jan/2026:08:12:06 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 1930 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #317 | Severity: Low | Type: Isolated Anomaly (Score: 10414.4072)

Log Details:

syslog_ts: Jan 28 08:13:46 host: servernameabc process: httpd[12345] ip1: 10.233.101.216 ip2: 0.1.0.1 session_id: 30620 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:46 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 404 bytes: - response_time: 633 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

Anomaly Detection Report

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #324 | Severity: Low | Type: Isolated Anomaly (Score: 10418.6055)

Log Details:

syslog_ts: Jan 28 08:13:52 host: servernameabc process: httpd[12345] ip1: 10.66.6.194 ip2: 0.1.0.1 session_id: 75928 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:52 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 404 bytes: - response_time: 1953 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #340 | Severity: Low | Type: Isolated Anomaly (Score: 10416.7070)

Log Details:

syslog_ts: Jan 28 08:14:02 host: servernameabc process: httpd[12345] ip1: 10.254.151.228 ip2: 0.1.0.1 session_id: 97303 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:02 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 404 bytes: - response_time: 1247 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #404 | Severity: Low | Type: Isolated Anomaly (Score: 10.1872)

Log Details:

syslog_ts: Jan 28 08:14:51 host: servernameabc process: httpd[12345] ip1: 10.97.177.26 ip2: 0.1.0.1 session_id: 52318 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:51 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 457 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #465 | Severity: Low | Type: Isolated Anomaly (Score: 22962.8457)

Log Details:

syslog_ts: Jan 28 08:15:28 host: servernameabc process: httpd[12345] ip1: 10.244.103.132 ip2: 0.1.0.1 session_id: 56141 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:28 +0530 request: GET /dashboard/stats HTTP/1.1 status: 503 bytes: - response_time: 671 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)

AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #478 | Severity: Low | Type: Isolated Anomaly (Score: 17.8127)

Log Details:

syslog_ts: Jan 28 08:15:38 host: servernameabc process: httpd[12345] ip1: 10.161.95.11 ip2: 0.1.0.1 session_id: 61523 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:38 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 1690 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #482 | Severity: Low | Type: Isolated Anomaly (Score: 22964.4844)

Log Details:

syslog_ts: Jan 28 08:15:42 host: servernameabc process: httpd[12345] ip1: 10.169.50.141 ip2: 0.1.0.1 session_id: 12979 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:42 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 503 bytes: - response_time: 1015 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #486 | Severity: Low | Type: Isolated Anomaly (Score: 10416.3711)

Log Details:

syslog_ts: Jan 28 08:15:46 host: servernameabc process: httpd[12345] ip1: 10.216.174.36 ip2: 0.1.0.1 session_id: 57414 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:46 +0530 request: GET /favicon.ico HTTP/1.1 status: 404 bytes: - response_time: 1134 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #627 | Severity: Low | Type: Isolated Anomaly (Score: 10418.9893)

Log Details:

syslog_ts: Jan 28 08:17:31 host: servernameabc process: httpd[12345] ip1: 10.77.151.96 ip2: 0.1.0.1 session_id: 75268 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:31 +0530 request: POST

Anomaly Detection Report

/api/v1/auth/login HTTP/1.1 status: 404 bytes: - response_time: 2160 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #658 | Severity: Low | Type: Isolated Anomaly (Score: 13.8432)

Log Details:

syslog_ts: Jan 28 08:17:57 host: servernameabc process: httpd[12345] ip1: 10.0.246.37 ip2: 0.1.0.1 session_id: 35400 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:57 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 530 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #665 | Severity: Low | Type: Isolated Anomaly (Score: 10415.0986)

Log Details:

syslog_ts: Jan 28 08:18:02 host: servernameabc process: httpd[12345] ip1: 10.109.113.19 ip2: 0.1.0.1 session_id: 99567 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:02 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 404 bytes: - response_time: 725 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #721 | Severity: Low | Type: Isolated Anomaly (Score: 17.9808)

Log Details:

syslog_ts: Jan 28 08:18:45 host: servernameabc process: httpd[12345] ip1: 10.229.137.70 ip2: 0.1.0.1 session_id: 76965 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:45 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 1768 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #782 | Severity: Low | Type: Isolated Anomaly (Score: 22962.4746)

Log Details:

syslog_ts: Jan 28 08:19:31 host: servernameabc process: httpd[12345] ip1: 10.246.136.183 ip2: 0.1.0.1 session_id: 84275 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:31 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 503 bytes: - response_time: 598 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #808 | Severity: Low | Type: Isolated Anomaly (Score: 22518.2793)

Log Details:

syslog_ts: Jan 28 08:19:51 host: servernameabc process: httpd[12345] ip1: 10.21.111.127 ip2: 0.1.0.1 session_id: 62248 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:51 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 500 bytes: - response_time: 4875 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #822 | Severity: Low | Type: Isolated Anomaly (Score: 22513.4668)

Log Details:

syslog_ts: Jan 28 08:20:04 host: servernameabc process: httpd[12345] ip1: 10.81.215.231 ip2: 0.1.0.1 session_id: 58271 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:04 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 500 bytes: - response_time: 1539 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #845 | Severity: Low | Type: Isolated Anomaly (Score: 22963.4922)

Log Details:

syslog_ts: Jan 28 08:20:19 host: servernameabc process: httpd[12345] ip1: 10.170.183.224 ip2: 0.1.0.1 session_id: 24418 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:19 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 503 bytes: - response_time: 816 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly Detection Report

Anomaly #919 | Severity: Low | Type: Isolated Anomaly (Score: 10418.9629)

Log Details:

syslog_ts: Jan 28 08:21:14 host: servernameabc process: httpd[12345] ip1: 10.229.153.128 ip2: 0.1.0.1 session_id: 26493 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:14 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 404 bytes: - response_time: 2145 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #959 | Severity: Low | Type: Isolated Anomaly (Score: 22512.7695)

Log Details:

syslog_ts: Jan 28 08:21:45 host: servernameabc process: httpd[12345] ip1: 10.180.11.40 ip2: 0.1.0.1 session_id: 41151 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:45 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 500 bytes: - response_time: 1183 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.

Anomaly #988 | Severity: Low | Type: Isolated Anomaly (Score: 10416.2783)

Log Details:

syslog_ts: Jan 28 08:22:08 host: servernameabc process: httpd[12345] ip1: 10.173.245.225 ip2: 0.1.0.1 session_id: 31417 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:08 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 404 bytes: - response_time: 1028 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

N/A

Reason for Detection:

Isolated anomaly (noise). Did not cluster with others.
